

203P1336W000

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2000-187935

(P 2 0 0 0 - 1 8 7 9 3 5 A)

(43) 公開日 平成12年7月4日 (2000.7.4)

(51) Int. Cl. ⁷	識別記号	F I	テーマコード (参考)
G11B 20/10		G11B 20/10	H
G06F 12/14	320	G06F 12/14	320 F

審査請求 未請求 請求項の数12 O L (全27頁)

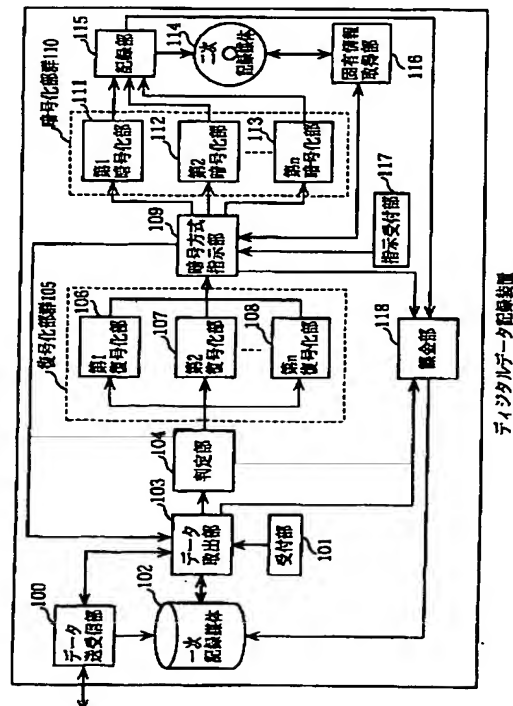
(21) 出願番号	特願平11-202971	(71) 出願人	000005821 松下電器産業株式会社 大阪府門真市大字門真1006番地
(22) 出願日	平成11年7月16日 (1999.7.16)	(72) 発明者	田川 健二 大阪府門真市大字門真1006番地 松下電器産業株式会社内
(31) 優先権主張番号	特願平10-206967	(72) 発明者	南 賢尚 大阪府門真市大字門真1006番地 松下電器産業株式会社内
(32) 優先日	平成10年7月22日 (1998.7.22)	(72) 発明者	小塚 雅之 大阪府門真市大字門真1006番地 松下電器産業株式会社内
(33) 優先権主張国	日本 (J P)	(74) 代理人	100090446 弁理士 中島 司朗 (外1名)
(31) 優先権主張番号	特願平10-289831		
(32) 優先日	平成10年10月12日 (1998.10.12)		
(33) 優先権主張国	日本 (J P)		

(54) 【発明の名称】 デジタルデータ記録装置及びその方法並びにそのプログラムを記録したコンピュータ読み取り可能な記録媒体

(57) 【要約】

【課題】 著作権を保護し、暗号化されたデジタルデータの再生を容易にするデジタルデータ記録装置を提供する。

【解決手段】 データ送受信部100は、電子配信される暗号化されたデジタルデータを受信し、一次記録媒体に記録する。データ取出部103で取り出されたデジタルデータは、判定部104で暗号形式が判定され、適切な一の復号化部で復号される。固有情報取得部116は、二次記録媒体114が再生装置に対して着脱可能か否かで二次記録媒体114又は再生装置の識別情報を取得する。暗号方式指示部109は、取得された識別情報に従い、複数の暗号化部から一の暗号化部を選ぶ。一の暗号化部は、識別情報を基に暗号鍵を生成し、デジタルデータを暗号化する。それを記録部115は二次記録媒体114に記録し、課金部118は、課金情報に従い課金する。



【特許請求の範囲】

【請求項 1】 デジタルデータを記録媒体に記録するデジタルデータ記録装置において、暗号化されたデジタルデータをデジタルネットワークを介して受信する通信手段と、前記通信手段により受信された暗号化デジタルデータを復号する復号化手段と、複数の暗号化部を有し、当該暗号化部はそれぞれ異なるセキュリティレベルを有する暗号化方式の一つでデジタルデータを暗号化する暗号化手段と、前記暗号化手段により暗号化されたデジタルデータを前記記録媒体に記録する記録手段と、前記復号化手段と前記暗号化手段とを制御する制御手段とを備え、

前記制御手段は、前記複数の暗号化部の一つで、前記復号化手段により復号化されたデジタルデータを再暗号化させることを特徴とするデジタルデータ記録装置。

【請求項 2】 前記記録媒体に記録されたデジタルデータは、再生装置により再生され、

前記暗号化手段は、前記記録媒体の識別情報を基に生成した暗号鍵によりデジタルデータを暗号化する第 1 暗号化部と、前記再生装置の識別情報を基に生成した暗号鍵によりデジタルデータを暗号化する第 2 暗号化部とを有し、前記制御手段は、

前記記録媒体が再生装置から着脱可能か否かを判定し、着脱可能なときは、前記第 1 暗号化部によりデジタルデータの暗号化を行わせ、着脱不可能なときは、前記第 2 暗号化部によりデジタルデータの暗号化を行わせることを特徴とする請求項 1 に記載のデジタルデータ記録装置。

【請求項 3】 前記デジタルデータ記録装置は、更に、前記デジタルネットワークを介して課金処理を行う課金手段を備え、

前記制御手段は、再暗号化を行う前記暗号化部の選択に基づいて課金値を決定し、決定した課金値に基づき課金処理を行うように前記課金手段を制御することを特徴とする請求項 1 に記載のデジタルデータ記録装置。

【請求項 4】 前記記録媒体に記録されたデジタルデータは、再生装置により再生され、前記暗号化手段は、前記記録媒体の識別情報を基に生成した暗号鍵によりデジタルデータを暗号化する第 1 暗号化部と、前記再生装置の識別情報を基に生成した暗号鍵によりデジタルデータを暗号化する第 2 暗号化部とを有し、前記制御手段は、前記記録媒体が再生装置から着脱可能か否かを判定し、着脱可能なときは、前記第 1 暗号化部によりデジタルデータの暗号化を行わせ、着脱不可能なときは、前記第

2 暗号化部によりデジタルデータの暗号化を行わせることを特徴とする請求項 3 に記載のデジタルデータ記録装置。

【請求項 5】 前記制御手段は、前記暗号化手段が前記暗号鍵を生成できない場合は、受信された暗号化デジタルデータを、前記復号化手段により復号化することを禁止することを特徴とする請求項 4 に記載のデジタルデータ記録装置。

【請求項 6】 前記暗号化手段の有する複数の暗号化部による暗号化されたデジタルデータは、前記通信手段により受信されたデジタルデータの暗号化に比べいずれもセキュリティレベルが低いことを特徴とする請求項 1 に記載のデジタルデータ記録装置。

【請求項 7】 前記通信手段により受信されるデジタルデータは異なるセキュリティレベルを有する暗号化方式の一つで暗号化されており、前記受信されるデジタルデータは当該デジタルデータの暗号化方式を示す属性情報を含み、

前記復号化手段は、複数の復号化部を含み、当該復号化部は前記異なるセキュリティレベルを有する暗号化方式で暗号化されたデジタルデータをそれぞれ復号化し、前記制御手段は、前記通信手段により受信された暗号化デジタルデータの暗号化方式を前記属性情報に基づいて判定し、判定した暗号化方式に対応する前記復号化部により前記暗号化デジタルデータを復号化するように前記復号化手段を制御することを特徴とする請求項 1 に記載のデジタルデータ記録装置。

【請求項 8】 前記デジタルデータ記録装置は、更に、

前記デジタルネットワークを介して課金処理を行う課金手段を備え、

前記制御手段は、受信した暗号化デジタルデータに対し、復号化を行う前記復号化部の選択と再暗号化を行う前記暗号化部の選択とに基づいて課金値を決定し、決定した課金値に基づき課金処理を行うように前記課金手段を制御することを特徴とする請求項 7 に記載のデジタルデータ記録装置。

【請求項 9】 デジタルデータを記録媒体に記録するデジタルデータ記録方法において、暗号化されたデジタルデータをデジタルネットワークを介して受信する通信ステップと、前記通信ステップにより受信された暗号化デジタルデータを復号する復号化ステップと、複数の異なるセキュリティレベルを有する暗号化方式の一つで復号化されたデジタルデータを暗号化する暗号化ステップと、前記暗号化ステップにより暗号化されたデジタルデータを前記記録媒体に記録する記録ステップとを備えることを特徴とするデジタルデータ記録方法。

【請求項 10】 前記通信ステップにより受信されるデ

デジタルデータは異なるセキュリティレベルを有する暗号化方式の一つで暗号化されており、前記受信されるデジタルデータは当該デジタルデータの暗号化方式を示す属性情報を含み、

複数の暗号化方式から一の暗号化方式を前記属性情報に基づいて判定する判定ステップを更に有し、

前記復号化ステップは、前記判定ステップに従い暗号化されたデジタルデータを復号化することを特徴とする請求項 9 に記載のデジタルデータ記録方法。

【請求項 11】 デジタルデータを第 1 記録媒体に記録するデジタルデータ記録装置に適用されるコンピュータ読み取り可能な記録媒体において、

暗号化されたデジタルデータをデジタルネットワークを介して受信する通信ステップと、

前記通信ステップにより受信された暗号化デジタルデータを復号する復号化ステップと、

複数の異なるセキュリティレベルを有する暗号化方式の一つで復号化されたデジタルデータを暗号化する暗号化ステップと、

前記暗号化ステップにより暗号化されたデジタルデータを前記第 1 記録媒体に記録する記録ステップとの各ステップをコンピュータに実行させるプログラムを記録したコンピュータ読み取り可能な記録媒体。

【請求項 12】 前記通信ステップにより受信されるデジタルデータは異なるセキュリティレベルを有する暗号化方式の一つで暗号化されており、前記受信されるデータは当該データの暗号化方式を示す属性情報を含み、複数の暗号化方式から一の暗号化方式を前記属性情報に基づいて判定する判定ステップを更に有し、

前記復号化ステップは、前記判定ステップに従い暗号化されたデジタルデータを復号化することをコンピュータに実行させるプログラムを記録した請求項 11 に記載のコンピュータ読み取り可能な記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、デジタルデータの著作権保護を図るデジタルデータ記録装置及びその方法並びにコンピュータ読み取り可能な記録媒体に関する。

【0002】

【従来の技術】近年のインターネットの普及により、PC（パーソナルコンピュータ）を用いて、ホームページ上から好みの音楽データなどをダウンロードにより入手し、クレジットカードなどの決済手段を通じて支払いを行う、いわゆるEC(ElectronicCommerce:電子商取引)による音楽流通が広がりつつある。このようなインターネットを通じたECによる音楽流通（以下「電子音楽配信」という。）が普及することは、ユーザがレコード店に行く必要がなくなることを意味し、現在のCD(Compact Disc)中心の音楽流通を大きく変えるものになる可能性を

持っている。

【0003】ところで、音楽を鑑賞するスタイルという点に注目すると、自宅で鑑賞する以外にも、携帯型の再生装置を用いて、通勤、通学途中に鑑賞する、あるいは車の中で鑑賞するというスタイルもかなりの割合を占める。この場合には、音楽データをMD(Mini Disc)等の可搬型の媒体に記録する必要がある。また、電子音楽配信においては、各社それぞれ独自の暗号方式を採用し、著作権保護を図っている。すなわち、製作会社、流通経路、利用形態等に応じて、それぞれ異なる暗号方式を採用している。

【0004】

【発明が解決しようとする課題】このような状況において、電子音楽配信によって音楽データをMD等に記録する場合、流通段階での音楽データをそのまま記録したとき、MD等を再生する再生装置は、各暗号方式に対応して復号化できる装置が求められる。この結果、装置規模が大きくなり、価格の上昇を招き、ユーザにとっては不利益となる。

【0005】一方、ユーザの利益だけを考えるなら、電子音楽配信された音楽データの暗号を復号化してMD等に記録するようにすれば、再生装置は、暗号解読を必要としないので安価なものを提供できることになる。しかしながら、この場合には、不正なコピーを助長して著作権保護を図ることができない。本発明は、上記課題に鑑みなされたものであり、著作権保護を図り、かつ記録媒体に記録された音楽データを安価なデジタルデータ再生装置で再生することができるデジタルデータ記録装置及びその方法並びにコンピュータ読み取り可能な記録媒体を提供することを目的とする。

【0006】

【課題を解決するための手段】上記課題を解決するために、本発明は、デジタルデータを記録媒体に記録するデジタルデータ記録装置において、暗号化されたデジタルデータをデジタルネットワークを介して受信する通信手段と、前記通信手段により受信された暗号化デジタルデータを復号する復号化手段と、複数の暗号化部を有し、当該暗号化部はそれぞれ異なるセキュリティレベルを有する暗号化方式の一つでデジタルデータを暗号化する暗号化手段と、前記暗号化手段により暗号化されたデジタルデータを前記記録媒体に記録する記録手段と、前記復号化手段と前記暗号化手段とを制御する制御手段とを備え、前記制御手段は、前記複数の暗号化部の一つで、前記復号化手段により復号化されたデジタルデータを再暗号化させることとしている。

【0007】

【発明の実施の形態】以下、本発明に係るデジタルデータ記録装置の実施の形態について図面を用いて説明する。

（実施の形態 1）図 1 は、本発明に係るデジタルデー

タ記録装置の実施の形態1の構成図である。このデジタルデータ記録装置は、データ送受信部100と、受付部101と、一次記録媒体102と、データ取出部103と、判定部104と、復号化部群105と、暗号方式指示部109と、暗号化部群110と、二次記録媒体114と、記録部115と、固有情報取得部116と、指示受付部117と、課金部118とを備えている。

【0008】なお、このデジタルデータ記録装置の二次記録媒体114と記録部115以外は、一般には図2に示すようにPC（パーソナルコンピュータ）201で実現され、記録部115は、例えばDVD(Digital Versatile Disc)-RAMドライブ202で、二次記録媒体114は、DVD-RAMディスク203でそれぞれ実現される。

【0009】このデジタルデータ記録装置は、インターネットを介して配信される暗号化されたデジタルデータである音楽データを受信し、一次記録媒体102にダウンロードした後、復号化部群105でデジタルデータを復号化し、暗号化部群110で再度暗号化したデジタルデータとして、記録部115で二次記録媒体114に記録する。

【0010】なお、本実施の形態では、電子音楽配信について説明するけれども、デジタルデータの種類は、音楽データに限るものではなく、映像データ、文字データあるいはこれらの組み合わせでもよい。データ送受信部100は、モデムと制御ソフトで実現される通信部であり、電話回線を通じて情報提供者のホストコンピュータ（図示せず）に接続される。受付部101で受け付けられた希望する曲の購入要求をデータ取出部103を介して通知されると、ホストコンピュータに送信する。インターネットを介して、ホストコンピュータから購入要求に従い配信される音楽データをダウンロードし、一次記録媒体102に記録する。また、曲を購入したときに生じる課金情報をホストコンピュータに送信する。

【0011】ここで、情報提供者が提供する情報について説明する。情報提供者は、曲販売のサイト、すなわち自社のホームページを開設しており、曲名、価格などユーザの購入時に必要な情報、あるいは購買意欲をかきたてる情報を提供している。ユーザは、これらの情報提供者が提供する情報に基づいて、好みの曲を購入する。図3は、情報提供者が提供する情報、すなわち曲販売用のホームページの一例を示すものである。表示される情報としては、曲名301、歌手名302、収録時間303、価格304などの内容からなる。ここで、曲名301、歌手名302は、それぞれ、個々の音楽データの曲名、歌手名を表す情報である。収録時間303は、個々の曲の収録時間（再生時間）を示し、価格304は、個々の曲の販売価格を示している。これらの情報をもとに、ユーザは受付部101を通じて好みの曲を選択し、購入要求を通知することができる。もちろん、情報提供

者が提供する情報は、図3に示すように、文字情報に限られるものではなく、ジャケットピクチャのような画像や、試聴用の音楽データであってもよいことは言うまでもない。

【0012】受付部101は、キーボードやマウス等からなり、PCの表示画面に表示された図3に示した情報を見たユーザから音楽データの購入要求を受け付ける。受け付けた曲の購入要求は、データ取出部103を介して、データ送受信部100に通知される。一次記録媒体102は、一般にはPCのハードディスク等で実現され、データ送受信部100で受信された暗号化されたデジタルデータである音楽データを記憶している。また、一次記録媒体のセキュアな領域には、課金部118によって、ダウンロードされた音楽データを二次記録媒体114に記録したとき、例えば暗号化した課金データが記録される。

【0013】図4は、一次記録媒体102に記憶されているダウンロードした音楽データ、すなわち情報提供者が提供する音楽データのデータ構造の一例を示すものである。情報提供者が提供する音楽データは、大きく音楽データの曲名や歌手名、価格などの情報である属性情報401と、音楽データそのものである曲データ部402とから構成される。

【0014】属性情報401は、ISRC情報403、曲名404、歌手名405、価格406、情報提供者名407、暗号形式408から構成される。以下、これらの属性情報について説明する。ISRC(International Standard Recording Code)情報403は、音楽データごとに割り当てられる固有の情報であって、国コード（2つのASCII文字）、オーナーコード（3つのASCII文字）、記録年（数字2桁）、シリアル番号（数字5桁）で構成される。曲名404、歌手名405は、それぞれ音楽データの曲名、歌手名を表す文字情報である。価格406は、音楽データの価格を表す情報である。なお、本実施の形態では、ダウンロードした音楽データをデジタルデータ記録装置を用いて、二次記録媒体に記録したときに請求される金額を示している。

【0015】情報提供者名407は、音楽データの提供者名、あるいは著作権者名を示す情報である。つまり、ユーザが本デジタルデータ記録装置を用いて音楽データを記録したときに課金し、その金額をどの業者に振り分ければよいのかを示す情報である。暗号形式408は、ダウンロードした音楽データがどの暗号形式で暗号化されているかを示す情報である。すなわち音楽データは、情報提供者ごとに異なる暗号方式で暗号化されている。例えば、情報提供者A、情報提供者B、情報提供者Cが音楽データを提供する場合、情報提供者Aの提供する音楽データはA方式で暗号化されており、情報提供者Bの提供する音楽データはB方式で暗号化されており、情報提供者Cの提供する音楽データはC方式で暗号化さ

れている。なお、本実施の形態では、情報提供者の提供する情報が、さまざまな形式で暗号化されている場合に、それを記録した二次記録媒体 114 を再生装置で著作権の保護を図りつつ、容易に解読できる暗号形式に変換することが発明の主たる目的であり、暗号化のアルゴリズムの詳細な説明については省略する。

【0016】また、属性情報 401 においては、価格 406、情報提供者名 407 は改竄されると情報提供者が不利益を被るおそれがあるため、必要に応じて暗号化されている。データ取出部 103 は、暗号方式指示部 109 からデジタルデータの取り出し指示を受けると、一次記録媒体 102 から、まず属性情報 401 を取り出し、属性情報 401 を課金部 118 に通知する。また、属性情報 401 中の暗号形式 408 の情報は、判定部 104 に通知する。なお、属性情報 401 中、価格 406 等が暗号化されているときは、復号化部群 105 によって、復号化してから課金部 118 に通知する。さらに一次記録媒体 102 から曲データ部 402 を取り出し、判定部 104 に出力する。データ取出部 103 で取り出されたデータは、すでに述べたように、情報提供者ごとに異なる暗号方式で暗号化されている。

【0017】判定部 104 は、データ取出部 103 から通知された暗号形式 408 の情報に基づいて、復号化部群 105 のいずれの復号化部に音楽データを出力するか判定する。復号化部群 105 は、 n 個の復号化部よりなり、第 1 復号化部 106 は A 方式で暗号化されたデジタルデータを復号し、第 2 復号化部 107 は B 方式で暗号化されたデジタルデータを復号し、第 n 復号化部 108 は N 方式で暗号化されたデジタルデータを復号する。各復号化部 106 ~ 108 は、情報提供者ごとの復号モジュールからなっている。

【0018】例えば、判定部 104 に通知された暗号形式 408 の情報が B 方式であれば、判定部 104 は、音楽データの曲データ部 402 のデジタルデータを第 2 復号化部 107 に出力し、復号する。第 2 復号化部 107 は、入力されたデジタルデータを復号して、暗号方式指示部 109 に出力する。第 1 から第 n 復号化部 106 ~ 108 のいずれかにより暗号化されたデータを復号する際、復号鍵が必要であればデータ送受信部 100 でデータの暗号方式に応じた復号鍵を入手し、データを復号化する。このようにして情報提供者ごとに異なる暗号方式で暗号化されているデータに対し、いったん各方式で暗号化されているデータを復号化する。

【0019】暗号方式指示部 109 は、指示受付部 117 から暗号方式の種類の指示を受けているときは、その指示に従った固有情報の取得を固有情報取得部 116 に指示する。固有情報取得部 116 から指示した固有情報の通知を受けたときは、データ取出部 103 に音楽データの取り出しを指示する。固有情報取得部 116 から指示に従った固有情報を取得できない旨の通知を受けたと

きには、表示部（図示せず）に指示された暗号方式の種類では暗号化できない旨を表示させる。また、指示受付部 117 から暗号方式の種類の指示を受けていないときには、固有情報取得部 116 に二次記録媒体 114 の属性に従った固有情報の取得を指示する。固有情報取得部 116 から固有情報又は固有情報を取得できない旨を通知されると、データ取出部 103 に音楽データの取り出しを指示する。固有情報を取得できない旨の通知を受けたときには、乱数を発生する。

【0020】暗号方式指示部 109 は、指示受付部 117 から暗号方式の指示を受け付けているときは、その指示に応じた一の暗号化部を選び、復号化部群 105 のいずれかの復号化部 106、107、…、108 から復号されたデジタルデータの入力を受けると、固有情報取得部 116 から通知された固有情報とともに、復号されたデジタルデータを通知する。

【0021】また、暗号方式指示部 109 は、指示受付部 117 から指示を受け付けていないときには、固有情報取得部 116 から通知された固有情報の種類に従い、一の暗号化部を選び、復号化部群 105 のいずれかの復号化部 106 ~ 108 から復号されたデジタルデータの入力を受けると、固有情報とともにデジタルデータを通知する。固有情報取得部 116 から固有情報を取得できない旨の通知を受けているとき、発生させた乱数とともに、一の暗号化部にデジタルデータを通知する。

【0022】暗号化部群 110 は、 n 個の暗号化部 111、112、…、113 からなる。各暗号化部 111、112、…、113 は、異なる種類の暗号鍵によって、通知されたデジタルデータを暗号化する。例えば、第 1 暗号化部 111 は、二次記録媒体 114 の固有の識別情報を基に作成される暗号鍵で暗号化する。第 2 暗号化部 112 は、二次記録媒体 114 を再生する再生装置（図示せず）の固有の識別情報を基に作成される暗号鍵で暗号化する。第 n 暗号化部 113 は、乱数を基に作成される暗号鍵で暗号化する。暗号化部 111 ~ 113 で用いられる各暗号鍵のデータサイズは、一次記録媒体 102 に記憶されている暗号化されたデジタルデータの暗号鍵のデータサイズよりも小さく設定される。

【0023】二次記録媒体 114 に記録される暗号化されたデジタルデータの暗号鍵のデータサイズが小さいことは、このデジタルデータを解読する際の困難性が低いことを意味する。したがって、二次記録媒体 114 を再生する再生装置でのデジタルデータの復号化に要する構成が簡単化されることになり、再生装置のコスト減につながる。

【0024】例えば、指示受付部 117 からの指示がないときに、暗号方式指示部 109 が固有情報取得部 116 から二次記録媒体の識別情報の通知を受けているときには、第 1 暗号化部 111 に二次記録媒体の識別情報を通知する。第 1 暗号化部 111 は、その識別情報を基に

暗号鍵を作成し、暗号方式指示部 109 から通知された音楽データの属性情報 401 の暗号形式 408 を書き換えるとともに、曲データ部 402 を、生成した暗号鍵で暗号化する。暗号化したデジタルデータを記録部 115 に通知する。

【0025】また、暗号方式指示部 109 は、指示受付部 117 から二次記録媒体 114 を再生する再生装置（図示せず）の固有情報による暗号化の指示を受けると、固有情報取得部 116 に再生装置の固有の識別情報を取得するよう指示する。固有情報取得部 116 から再生装置の固有の識別情報を通知されると、その識別情報と復号化部群 105 から通知された復号されたデジタルデータとを第 2 暗号化部 112 に通知する。

【0026】第 2 暗号化部 112 は、暗号方式指示部 109 から通知された識別情報を基に暗号鍵を生成し、生成した暗号鍵でデジタルデータを暗号化して記録部 115 に通知する。この際、音楽データの属性情報 401 の暗号形式 408 の内容を書き換えるのは、指示受付部 117 から指示を受け付けなときと同様である。二次記録媒体 114 は、例えば図 2 に示した DVD-RAM ディスク、MD、再生装置（図示せず）の機種により埋め込み型あるいは取り外し可能な型の小型の半導体メモリ等からなり、暗号化部群 110 で暗号化された音楽データが記録部 115 によって記録される。例えば、DVD-RAM ディスク 203 にデジタルデータが記録されていれば、図 2 に示すように、DVD-Audio プレーヤ 204 に DVD-RAM ディスク 203 を挿入して音楽を聴取することができる。

【0027】記録部 115 は、例えば、図 2 に示した DVD-RAM ドライブ 202 で実現され、暗号化部群 110 から通知されたデジタルデータを二次記録媒体 114 に記録する。また、記録が終了すると、その旨、課金部 118 に通知する。固有情報取得部 116 は、暗号方式指示部 109 から二次記録媒体 114 の固有の識別情報の取得を指示されたときには、例えば、DVD-RAM の場合は BCA (Burst Cutting Area) に書かれている情報を読み出し、通知する。なお、この二次記録媒体 114 の固有の識別情報は、媒体ごとにユニークであり、通常ディスクの製造時に記録される情報であって、ユーザの通常の操作では読み出されたり、書き換えることができない。

【0028】したがって、この識別情報を基に暗号鍵を生成して、この暗号鍵で暗号化されたデジタルデータが DVD-RAM ディスクに記録されるので、万一悪意を持ったユーザがビットコピー可能なツールを用いて DVD-RAM ディスクの内容を複製し、再生しようとしても、復号鍵の基になる情報が異なるため、正常に復号化することができない。この結果、音楽データの著作権を確実に保護することができる。

【0029】また、暗号方式指示部 109 から二次記録媒体 114 が装着された再生装置（図示せず）の固有の

識別情報の取得を指示されたときには、固有情報取得部 116 は、再生装置の識別情報を読み出し、暗号方式指示部 109 に通知する。この再生装置の固有の識別情報も再生装置の製造時に付される装置ごとのユニークな識別情報であるので、ユーザの通常の操作では読み出されたり、書き換えられたりすることはできない。したがって、この識別情報を基に暗号化された場合も、特定の再生装置でしか再生することができない。

【0030】なお、固有情報取得部 116 は、暗号方式指示部 109 から指示された固有の識別情報を取得できないとき、即ち、二次記録媒体 114 又は再生装置に識別情報が付されていない場合には、指示された種類の固有の識別情報を取得できない旨を暗号方式指示部 109 に通知する。固有情報取得部 116 は、暗号方式指示部 109 から固有情報の種類の指示を受けずに、固有情報の取得の指示を受けると、二次記録媒体 114 が DVD-RAM ディスクなどの再生装置から取り外し可能なものであるか、それとも、小型の半導体メモリのような再生装置に埋め込まれた取り外し不可能のものであるかを判断し、取り外し可能なものであれば、その二次記録媒体 114 の固有の識別情報を読み出し、暗号方式指示部 109 に二次記録媒体 114 の識別情報を通知し、取り外し不可能のものであれば、再生装置の識別情報を読み出し、同様に再生装置の識別情報を通知する。識別情報を取得できないときは、その旨を暗号方式指示部 109 に通知する。

【0031】指示受付部 117 は、PC のキーボードやマウスで実現され、ユーザから暗号方式の種類を指示を受け付け、暗号方式指示部 109 に通知する。先に述べた図 3 に示すホームページの情報では、販売価格は 1 通りしかなかったけれども、図 5 に示すようなホームページの内容であれば、価格 (1) 501、価格 (2) 502 の 2 通りの販売価格が示されている。

【0032】価格 (1) 501 は、二次記録媒体 114 の固有の識別情報を基にデジタルデータを暗号化して記録するときの価格を示しており、価格 (2) 502 は、二次記録媒体 114 を再生する再生装置の固有の識別情報を基にデジタルデータを暗号化して記録するときの価格を示している。なお、これらの 2 種類の価格は、情報提供者側でそれぞれ個別に自由に設定可能である。

【0033】ユーザは、指示受付部 117 から二次記録媒体 114 の利用形態に応じて、図 5 に示す曲情報あるいはその価格情報を参照して好みの暗号形態でデジタルデータを暗号化することを指示することができる。例えば、特定の再生装置でのみ再生するとき、即ち、他の再生装置で二次記録媒体 114 を再生しないときには、再生装置の固有の識別情報を基に暗号化することを指示する。図 5 に示すように再生装置の識別情報を基に暗号化するほうが、価格 (2) 502 に示すように一般的に

安価である。これは、他の再生装置で再生することができないので、二次記録媒体114の固有の識別情報を基に暗号化するよりも自由度が低いからである。ユーザは、自由に再生装置を選んで再生したいときには、二次記録媒体114の識別情報を基に暗号化するように指示すればよい。

【0034】なお、指示受付部117と上述の受付部101とは、一体として構成されているけれども、説明上、2つの構成要素として説明した。課金部118は、データ取出部103から音楽データの属性情報401の通知を受け、記憶している。記録部115から暗号化されたデジタルデータを二次記録媒体114に記録した旨の通知を受けると、属性情報中の価格406を参照して課金額を決定し、一次記録媒体102のセキュア領域に属性情報401とともに課金情報として書き込む。

【0035】なお、価格406が図5に示したように価格(1)501、価格(2)502のように複数あるときは、暗号方式指示部109から通知された第1から第n暗号化部111~113のいずれが利用されたかに従い課金額を決定する。次に、本実施の形態の動作を図6、図7のフローチャートを用いて説明する。まず、受付部101はユーザからのホームページ表示の要求を受け、データ送受信部100が音楽データを提供する情報提供者が開設するホームページにアクセスし、データ取出部103によって表示部(図性せず)にホームページ(図3、図5参照)を表示させる(S602)。

【0036】次に、データ取出部103は、受付部101からユーザの希望する音楽データの購入指示を待ち、指定された音楽データの配信を受けるようデータ送受信部100に指示する(S604)。データ送受信部100は、音楽データを受信すると、一次記録媒体102にダウンロードする(S606)。ユーザは、ホームページの表示をみて、暗号方式の種類を二次記録媒体114の利用形態に応じて、指示受付部117から入力する。

【0037】暗号方式指示部109は、指示受付部117から暗号方式の種類の指示を通知されたか否か判断し(S608)、通知されたときは、指示された暗号方式の種類に用いる固有情報の取得を固有情報取得部116に指示する(S610)。固有情報取得部116から指示された固有情報を取得できない旨の通知を受けたか否かを判断し(S612)、その旨の通知を受けたときは、指示された暗号方式の種類では暗号化できない旨を表示部(図性せず)に表示させ(S614)、処理を終了する。指示した種類の固有情報の通知を受けたときには、データ取出部103にデジタルデータの取り出しを指示する。

【0038】データ取出部103は、一次記録媒体102に記録されている音楽データを取り出す(S616)。S608において、暗号方式指示部109は、指示受付部117から指示を通知されないと判断したと

き、固有情報取得部116に固有情報の種類を指定しないで、固有情報の取得を指示する(S618)。

【0039】固有情報取得部116は、二次記録媒体114の属性(再生装置(図性せず)に装着された二次記録媒体114が取り外し可能か不可能か)を判断し、取り外し可能な二次記録媒体114のときは二次記録媒体114の識別情報を取得し、取り外し不可能な二次記録媒体114のときは再生装置の識別情報を取得する(S620)。

【0040】暗号方式指示部109は、固有情報取得部116から取得された固有(識別)情報又は、固有情報を取得できなかったときはその旨の通知を受けると(S622)、データ取出部103にデジタルデータの取り出しを指示し、S616に移る。次に、判定部104は、データ取出部103で取り出された音楽データの属性情報401中の暗号形式408を参照して、復号化部群105のいずれの復号化部106~108で復号するかを判定する(S702)。

【0041】判定部104で判定された一の復号化部は、判定部104を介して入力されたデジタルデータを復号化し、復号したデジタルデータを暗号方式指示部109に出力する(S704)。暗号方式指示部109は、既に固有情報取得部116から通知されている固有情報(取得できない旨の情報も含む)に従い、暗号化部群110の一の暗号化部を選び、固有情報(取得できない旨の情報に対しては発生した乱数)と復号化されたデジタルデータとを通知する(S706)。

【0042】暗号方式指示部109から通知を受けた一の暗号化部は、固有(識別)情報に基づいて暗号鍵を生成し(乱数の通知に対しては乱数に基づいて暗号鍵を生成し)、デジタルデータを暗号化する。この際、属性情報401のうち暗号形式408の内容も書き換えられる(S708)。記録部115は、第1~第n暗号化部111~113のいずれかから通知されたデジタルデータを二次記録媒体114に記録し(S710)、記録が終了すると課金部118に通知する。

【0043】課金部118は、記録部115から通知を受けると、データ取出部103から通知されている価格406等に従い課金額を決定し、課金情報を一次記録媒体102に記録して(S712)処理を終了する。上記実施の形態では、復号化部群105は、情報提供者ごとの復号モジュール(復号化部)からなるものとしたけれども、復号化部群は、音楽データの品質、例えば24ビットのLPCM(Liner Pulse Code Modulation)、MP3(Moving Picture Experts Group 1 Audio Layer 3)等のデジタルデータ、に応じて各復号化部を設けてもよい。高品質の24ビットのLPCMは、解読の困難性の高い暗号化されたデジタルデータとし、通常品質のMP3は解読の困難性の低い暗号化されたデジタルデータとしておき、第1復号化部は24ビットのLPCMの

デジタルデータを復号し、第2復号化部はMP3のデジタルデータを復号するようにしてもよい。

【0044】上記実施の形態では、暗号化部群110は、固有情報の種類で各暗号化部を設けたけれども、上述した品質に対応して、第1復号化部で復号化されたデジタルデータは第1暗号化部で暗号化し、第2復号化部で復号化されたデジタルデータは第2暗号化部で暗号化し、第n復号化部で復号化されたデジタルデータは第n暗号化部で暗号化するようにしてもよい。この場合、第1暗号化部で暗号化に用いる暗号鍵のデータサイズは、第2暗号化部のそれよりも大きく、第2暗号化部のそれは第n暗号化部のそれよりも大きく設定する。そして、課金部は、デジタルデータの復号化がされた複合化部と復号化されたデジタルデータを再暗号化がされた暗号化部とによって課金額を決定する。このようにすることによって、高品質の音楽データの方がより著作権の保護を確実なものとするができる。また、この際、価格についても情報提供者は高品質の音楽データに高価格を設定することができる。

【0045】なお、上記実施の形態のデジタルデータ記録装置は、図1にその構成図を示したけれども、各構成要素の機能をコンピュータに発揮させるプログラムをコンピュータ読み取り可能なフロッピーディスク等の記録媒体に記録しておき、著作権の保護機能を有しないデジタルデータ記録装置に摘要して著作権の保護機能を有する装置とすることができる。

【0046】また、本実施の形態では、デジタルデータはユーザが購入希望を出したときにホストコンピュータからダウンロードするとして説明を行ったが、購入するしないにかかわらず音楽データ、あるいは、属性情報のみをいったんユーザのPC内の一次記録媒体102に記録しておき、一次記録媒体102に記録されているデジタルデータに対して購入手続きを行う形態も考えられる。

【0047】また、本実施の形態では、属性情報401は曲データ402と別個に記述するとして説明を行ったが、いわゆるWater Mark（電子すかし）の形式で曲データ402のデジタルデータ中に埋め込むことも可能である。また、本実施の形態において、復号化部群105と暗号化部群110との間の暗号方式指示部109を介してのデータ入出力に関しては特に言及はしていないが、セキュリティ上、認証を行ってデータを送信するか、あるいは復号化部群105、暗号方式指示部109及び暗号化部群110を1つのチップで実現する、といった方法で復号化されたデータの漏洩を防ぐようにしてもよい。

【0048】また、課金情報を記録するときには、一次記録媒体102中のセキュアな領域に記録するとして説明を行ったが、課金情報に関しては、一次記録媒体102とは別のICカードなどの記録媒体を設け、これに記

録することが可能である。本実施の形態では、課金のタイミングについては、説明を省略したが、例えば、デジタルデータを二次記録媒体114に記録するときには必ずホストコンピュータと接続していなければいけないとするか、課金額が一定の金額に達するとホストコンピュータに自動的に接続するか、あるいは、課金情報記録後、一定の日時が経過すると自動的にホストコンピュータに接続する、としてもよい。

【0049】更に、本実施の形態では、情報提供者が提供する情報を音声情報として説明したが、これに限るものではなく、映像情報、音声情報、文字情報、あるいは、映像情報と音声情報と文字情報との組み合わせたものなどでもよいことはもちろんである。

（実施の形態2）図8は、本発明に係わるデジタルデータ記録装置の実施の形態2の構成図である。このデジタルデータ記録装置は、一般にはパーソナルコンピュータで実現され、データ送受信部2101、一次記録媒体2102、データ取出部2103、暗号方式判定部2104、第1の復号化部2105、第2の復号化部2106、第3の復号化部2107、暗号化部2108、記録部2109、二次記録媒体2110、入力部2111、表示部2112、記録媒体固有情報取得部2113を備える。また、復号化部群2115は、第1の復号化部2105、第2の復号化部2106、第3の復号化部2107から構成されるが、復号化部は3つに限るものではなく、ここでは、複数の復号化部から構成されることを示している。

【0050】なお、本実施の形態では、以後、記録対象となるデータを音楽データであるとし、音楽データはインターネットを通じて配信されるものとする。また、情報提供者ごとに異なる暗号方式でデータを暗号化しているものとする。情報提供者は、曲名、価格、コピー制御情報など（以後、属性情報と称する）購入時に必要な情報、あるいは購買意欲をかきたてる情報を音楽データに重畳または音楽データから分離して提供するものとするが、本実施の形態では、属性情報を音楽データから分離して提供する形態について説明する。

【0051】データ送受信部2101は、モデムで実現される通信部であり、電話回線を通じて提供者のホストコンピュータ（図示せず）に接続される。まず、ユーザは情報提供者が提供する属性情報を取得する。データ送受信部2101により取得した属性情報は、一次記録媒体2102に記録され、その一部または全部が表示部2112に表示される。図9は、表示部2112に表示される情報の一例を示すものである。表示される情報としては、曲名2201、曲名コード2202、歌手名2203、データ入手先2204などの内容からなる。ここで、曲名2201、歌手名2203は、それぞれ音楽データに対する曲名、歌手名を表す情報である。曲名コード2202は、音楽データを他の音楽データと識別する

ための識別子であり、例えば I S R C (International Standard Recording Code) 情報が付される。これらの情報をもとに、ユーザは入力部 2 1 1 1 を通じて好みの曲を選択し、購入要求を通知することができる。データ入手先 2 2 0 4 は、本実施の形態では該当する曲が記録されている URL (Uniform Resource Locator) 情報とする。もちろん、曲名コード 2 2 0 2 に I S R C 情報が付されていれば、曲名コード 2 2 0 2 からデータ入手先を特定することも可能である。

【0052】入力部 2 1 1 1 は、マウス、キーボード等から実現され、ユーザからの曲の購入の指示、すなわち記録指示を受け付け、データ送受信部 2 1 0 1 に通知する。ユーザは表示部 2 1 1 2 に表示された情報を元に、マウスでその曲名等をクリックして音楽データの記録を指示する。入力部 2 1 1 1 から音楽データの記録指示があると、データ送受信部 2 1 0 1 から電話回線を通じて提供者のホストコンピュータから記録要求のあった曲をダウンロードする。この際に、属性情報中の URL 情報をもとに曲データの位置を特定する。ダウンロードされたデータはいったん一次記録媒体 2 1 0 2 に記録される。

【0053】一次記録媒体 2 1 0 2 は、一般にはパソコンのハードディスクであって、ユーザが購入を希望した音楽データを暗号化されたまま記録する。したがって以後の動作に関しては、必ずしも常に提供者のホストコンピュータと接続している必要はない。データ取出部 2 1 0 3 は、一次記録媒体 2 1 0 2 から記録対象となる音楽データを取り出す。このとき、ユーザは表示部 2 1 1 2 に表示される図 9 に示した情報と同程度の情報をもとに、二次記録媒体 2 1 1 0 へ記録する音楽データを入力部 2 1 1 1 を通じて選択する。データ取出部 2 1 0 3 で取り出されたデータは、各情報提供者ごとの暗号方式で暗号化されている。このため、適当な復号方式で復号することを暗号方式判定部 2 1 0 4 により判定する。具体的には、デジタルデータのヘッダ部に暗号方式を識別できる情報を付加して送信する、属性情報に暗号方式を記述しておく、などの方法が考えられ、これらの値に応じて暗号方式を判定する。

【0054】第 1 の復号化部 2 1 0 5、第 2 の復号化部 2 1 0 6、第 3 の復号化部 2 1 0 7 は、各情報提供者ごとの復号方式が存在していることを示すものであって、必ずしも 3 つに限られるわけではない。暗号方式判定部 2 1 0 4 により適当な復号化部を選択し、復号化部により暗号化されたデータを復号する。このとき、例えば暗号方式判定部 2 1 0 4 で取得したデータの暗号方式に応じた復号鍵を入手または生成し、復号化部はこの復号鍵をもとにデータを復号化する。したがって、異なる暗号方式で暗号化されているデータに対し、いったん各方式で暗号化されているデータを復号化することになる。

【0055】次に、暗号化部 2 1 0 8 にて復号化された

データの暗号化を行うが、ここでは、記録媒体固有の固有情報を暗号鍵情報として暗号化を行うこととする。なお、記録媒体固有情報をもとに暗号化を行う一の方法については、特開平 5 - 2 5 7 8 1 6 公報に開示されているので、ここでは詳しい説明は省略する。記録媒体固有情報取得部 2 1 1 3 は、暗号化部 2 1 0 8 からの指示に従い、二次記録媒体 2 1 1 0 から固有情報を取り出し、暗号化部 2 1 0 8 へ伝達する。

【0056】暗号化部 2 1 0 8 は、記録媒体固有情報取得部 2 1 1 3 で取得した固有情報を暗号鍵として、暗号化する。ここで、二次記録媒体 2 1 1 0 固有の情報について説明する。二次記録媒体 2 1 1 0 は、媒体ごとの固有の識別情報を持っている。これは例えば DVD-RAM (Digital Versatile Disc Random Access Memory) の場合、BCA (Burst Cutting Area) に書かれた情報に相当する。この情報は、ディスクごとにユニークであり、しかも通常ディスク製作時に記録される情報であって、書き換えることができない。したがって、万一悪意を持ったユーザがビットコピー可能なツールを用いてディスクの内容を複製したとしても、復号鍵のもとになる情報が異なるために復号化することができず、データの著作権を確実に保護することが可能となる。

【0057】記録部 2 1 0 9 は、暗号化されたデータを二次記録媒体 2 1 1 0 に記録する。以上のように構成されたデジタルデータ記録装置について、以後図 10 のフローチャートを用いてその動作を説明する。まず、データ送受信部 2 1 0 1 は、属性情報をダウンロードし

(S 2 3 0 1)、ユーザからのデジタルデータの記録指示を待ち (S 2 3 0 2)、指示されたデジタルデータをダウンロードし、一次記録媒体 2 1 0 2 に記録する (S 2 3 0 3)。次に、ダウンロードしたデータの暗号方式を判定し、適当な復号化部 2 1 0 5 ~ 2 1 0 7 へ復号化を指示する (S 2 3 0 4)。復号化部 2 1 0 5 ~ 2 1 0 7 により復号化する (S 2 3 0 5)。暗号化部 2 1 0 8 は、復号化されたデータが入力されると、記録媒体固有情報取得部 2 1 1 3 から二次記録媒体 2 1 1 0 の固有情報を取得する (S 2 3 0 6)。取得した固有情報を暗号鍵の一部として暗号鍵を作成し、暗号化部 2 1 0 8 はデータを暗号化する (S 2 3 0 7)。記録部 2 1 0 9 は、暗号化されたデータを二次記録媒体 2 1 1 0 に記録し (S 2 3 0 8)、処理を終了する。

【0058】以上で、本発明の実施の形態 2 のデジタルデータ記録装置に関する説明を終わる。次に、本発明の実施の形態 3 のデジタルデータ記録装置に関する説明を行う。

(実施の形態 3) 図 11 は、本発明に係わるデジタルデータ記録装置の実施の形態 3 の構成図である。このデジタルデータ記録装置は、一般にはパーソナルコンピュータで実現され、データ送受信部 2 1 0 1、一次記録媒体 2 1 0 2、データ取出部 2 1 0 3、暗号方式判定部

2104、復号化部群2115、属性情報取得部2401、コピー制御情報検出判定部2402、コピー制御情報変換部2403、課金情報算出部2404、暗号化部2108、記録部2109、二次記録媒体2110、入力部2111、表示部2112、記録媒体固有情報取得部2113を備える。

【0059】なお、実施の形態3では、実施の形態2のデジタルデータ記録装置の各構成部分と同一の部分には同一の符号を付して、その説明を省略し、本実施の形態固有の部分について説明する。まず、本実施の形態において、記録対象となるデータの属性情報が図12の通りであるとする。図12に示す属性情報は、図9に示す属性情報に加えて、コピー制御情報2501、課金情報2502等の情報がある。ここで、コピー制御情報2501は、コピーが許可されている世代数、あるいは回数の情報からなる。例えば世代数に関しては、「無制限にコピー可」、「1世代だけコピー可(孫コピー禁止)」、「コピー禁止」等の値を取る。一方、回数に関しては、コピー許可されている回数の中で、0以上の整数値を取りうる。例えば「孫コピー不可」は、二次記録媒体2110にデジタルデータを記録後、二次記録媒体2110中のデータをもとにコピーすることを許可しないことを意味する。「無制限に許可」は、特に制限しないことを意味する。「2回コピー可」など、コピーの回数の情報が含まれる場合は、二次記録媒体2110に記録できる回数を意味する。

【0060】属性情報取得部2401は、一次記録媒体2102から、再生すべきデータに対応する属性情報を取得する。ここでは、コピー制御情報と課金情報を取り出す。なお、属性情報は著作権保護情報や課金情報を含むので、一次記録媒体2102中のセキュアな領域に記録して、ユーザの通常の操作ではアクセスできないことが望ましい。

【0061】コピー制御情報検出判定部2402は、属性情報中のコピー制御情報を取り出し、以後のコピーが許可されているかどうか、許可されているとすればその世代数、あるいは回数の情報を取得する。コピー制御情報検出判定部2403は、コピーが許可されている場合、コピー制御情報を必要に応じて書き換える。例えば、孫コピーが禁止されているときは、コピー制御情報の値を以後のコピーを禁止するように変更し、コピー許可回数が制限されているときは、許可回数から「1」減じた値に変更する。

【0062】ここで重要となるのは、コピー許可回数が設定されているとき、一般に、一次記録媒体2102に記録されたデータを何回二次記録媒体2110にコピーさせるかという数値であるため、コピー制御情報の書き換え対象となるのは、一次記録媒体2102中に記録されているデータである。したがって、一次記録媒体2102中に記録されている。コピー許可回数を「1」減じ

た値に変換し、二次記録媒体2110に記録すべきコピー許可回数は0として記録する。

【0063】課金情報算出部2404は、属性情報取得部2401で取得した属性情報から該当する曲の課金情報を取得し、これをもとに課金額を算出し、一次記録媒体2102中のセキュアな領域に記録する。以上のように構成されたデジタルデータ記録装置について、以下、図13および図14のフローチャートを用いてその動作を説明する。

【0064】まず、データ送受信部2101は、属性情報をダウンロードし(S2601)、ユーザからのデジタルデータの記録指示を待ち(S2602)、指示されたデジタルデータをダウンロードし、一次記録媒体2102に記録する(S2603)。次に、記録対象となるデータの属性情報を属性情報取得部2401により取得する(S2604)。コピー制御情報判定部2402により属性情報中のコピー制御情報を判定し、コピーが許可されているかどうかを判定する(S2605)。コピーが許可されているときは、コピーが許可されている世代、回数の情報を取得し、必要に応じてコピー制御情報変換部2403で書き換える(S2606)。コピーが許可されていない場合は、以後の処理を中断する(S2607)。次に暗号化方式を判定し、復号化群2115中の適当な復号化部へ復号化を指示する(S2608)。復号化部2105~2107により復号化を行う(S2609)。復号化が終わると、属性情報取得部2401で取得した属性情報中の課金情報から適切な課金額を算出する(S2610)。

【0065】暗号化部2108は、復号化されたデータが入力されると、記録媒体固有情報取得部2113から二次記録媒体2110の固有情報を取得する(S2611)。取得した固有情報を暗号鍵の一部として暗号鍵を作成し、暗号化部2108はデータを暗号化する(S2612)。記録部2109は、暗号化されたデータを二次記録媒体2110に記録し(S2613)、処理を終了する。

【0066】以上で、本発明の実施の形態3に関する説明を終わる。

(実施の形態4) 次に、本発明に係わるデジタルデータ記録装置の実施の形態4について説明する。このデジタルデータ記録装置は、実施の形態2とほぼ同一であるが、固有情報取得送出处2803、記録部2109、二次記録媒体2110が第2のデジタルデータ記録装置内にある点と、暗号鍵の情報のみが異なる。図15は、本発明に係わるデジタルデータ記録装置の実施の形態4の構成図である。このデジタルデータ記録装置は、第1のデジタルデータ記録装置2800と、第2のデジタルデータ記録装置2801とからなる。

【0067】第1のデジタルデータ記録装置2800は、データ送受信部2101、一次記録媒体2102、

データ取出部 2103、暗号方式判定部 2104、復号化部群 2115、暗号化部 2108、入力部 2111、表示部 2112、固有情報取得部 2802 備える。第 2 のデジタルデータ記録装置 2801 は、固有情報取得送出部 2803、記録部 2109、二次記録媒体 2110 を備える。

【0068】なお、実施の形態 4 では、実施の形態 2 のデジタルデータ記録装置の各構成部分と同一の部分には同一の符号を付して、その説明を省略し、本実施の形態固有の部分について説明する。暗号化部 2108 へ復号化部群 2115 にて復号されたデータが入力されると、記録媒体固有情報取得部 2802 は、第 2 のデジタルデータ記録装置 2801 中の固有情報取得送出部 2803 へ固有情報の送出要求を出す。固有情報取得送出部 2803 は、第 2 のデジタルデータ記録装置 2801 に装着されている二次記録媒体 2110 の固有識別情報、あるいは第 2 のデジタルデータ記録装置 2801 固有の識別情報、あるいはその両方を取得し、固有情報取得部 802 へ送出する。

【0069】暗号化部 2108 では、第 2 のデジタルデータ記録装置 2801 に装着されている二次記録媒体 2110 の固有識別情報、あるいは第 2 のデジタルデータ記録装置 2801 固有の識別情報、あるいは、二次記録媒体 2110 の固有識別情報と第 2 のデジタルデータ記録装置 2801 固有の識別情報の組み合わせの情報を暗号鍵の一部としてデータを暗号化し、第 2 のデジタルデータ記録装置 2801 へ出力する。第 2 のデジタルデータ記録装置 2801 中の記録部 2109 は暗号化されたデータを二次記録媒体 2110 へ記録する。

【0070】なお、固有情報取得送出部 2803 で取得送出する固有情報であるが、二次記録媒体 2110 が第 2 のデジタルデータ記録装置 2801 に固定的に設けられているときは、装置固有の識別情報とし、二次記録媒体 2110 が着脱自在に設けられているときは、二次記録媒体 2110 固有の固有情報、あるいは二次記録媒体 2110 の固有識別情報と第 2 のデジタルデータ記録装置 2801 固有の識別情報の組み合わせの情報とすることにより、より柔軟な暗号方式を使用することが可能になる。

【0071】以上で、実施の形態 4 の説明を終わる。

(実施の形態 5) 次に、本発明に係わるデジタルデータ記録装置の実施の形態 5 について説明する。このデジタルデータ記録装置は、実施の形態 2、3 および 4 とほぼ同一である。ここでは、実施の形態 4 の説明に用いた構成図、図 15 を用いて説明する。相違点は、二次記録媒体 2110 に応じた暗号形式を採用し、記録することである。つまり、DVD-RAM と半導体メモリとでは取り扱うデータの最小単位、暗号化データを書きこむデータ量の単位の単位が異なるため、固有情報取得部 2802 は、固有情報取得送出部 2803 から、媒体の情報も取

得して、最適なデータの単位で暗号化を行なうことになる。このため、暗号化部 2108 が複数存在し、適切な暗号化部へ固有情報ならびに媒体情報も伝達するものである。以上より、DVD-RAM に限らず、半導体メモリ、I C カード、ハードディスク等を二次記録媒体 2110 として使用することが可能となる。

【0072】以上で、実施の形態 5 の説明を終わる。なお、上記実施の形態 2～5 は現状において最善の効果が期待できるシステム例として説明したにすぎない。本発明は、その要旨を逸脱しない範囲で実施変更することができる。具体的には以下に示すような変更実施が可能である。また、実施の形態 2～5 では、デジタルデータはユーザが購入希望を出したときにホストコンピュータからダウンロードするとして説明を行ったが、購入するしないにかかわらずいったんユーザの PC 内の一次記録媒体 2102 に記録しておき、一次記録媒体 2102 に記録されているデジタルデータに対して購入手続きを行う形態も考えられる。

【0073】また、実施の形態 2～5 では、コピー制御情報を属性情報に記述するとして説明を行なったが、いわゆる Water Mark (電子すかし) の形式でデジタルデータ中に埋め込むことも可能である。また、課金情報を記録するときには、一次記録媒体 2102 中のセキュアな領域に記録するとして説明を行なったが、課金情報に関しては、一次記録媒体 2102 とは別の IC カードなどの記録媒体を設け、これに記録することが可能である。

【0074】また、実施の形態 2～5 では、情報提供者が提供する情報を音声情報として説明したが、これに限るものでなく、映像情報、音声情報、文字情報、あるいは、映像情報と音声情報と文字情報の組み合わせたものなどでもよいことはもちろんである。

(実施の形態 6) 図 16 は、本発明に係るデジタルデータ記録装置の実施の形態 6 の構成図である。

【0075】このデジタルデータ記録装置は、通信部 3101 と、記録媒体 3102 と、受信データ記録判定部 3103 と、表示部 3104 と、入力操作部 3105 と、記録媒体固有情報取得部 3106 と、暗号化部 3107 と、記録部 3108 と、課金情報記録部 3109 と、課金情報記録媒体 3110 と、課金部 3111 とを備えており、PC で実現される。

【0076】通信部 3101 は、モデムで実現され、電話回線を介してデータ提供者のホストコンピュータ (図示せず) 及び課金センタ (図示せず) に接続される。ホストコンピュータからデジタルデータとその属性情報とを受信すると、受信データ記録判定部 3103 に通知する。また、通信部 3101 は、課金センタから利用料の問い合わせがあると、その旨課金部 3111 に通知し、課金部 3111 から課金情報の通知を受けると、電話回線を介して、課金センタに課金情報を通知する。

21

【0077】本実施の形態では、データ提供者が提供するデジタルデータを音楽データであるとして説明する。データ提供者は、提供する音楽データを必要に応じて暗号化したデジタルデータとし、デジタルデータには、情報識別子が付されている。情報識別子は、曲名コードであり、他の音楽と識別するためのものである。また、デジタルデータには、属性情報が付加されている。属性情報は、デジタルデータの利用料金等を示すものであり、どの情報提供者から提供された情報であるかを示す情報も含まれている。

【0078】図17は、属性情報の内容の一例を示す図である。属性情報3201には、デジタルデータの曲名3202、演奏者（歌手）3203、曲名コード3204、記録料金3205、1回あたりの再生料金3206、再生可能回数3207、暗号状態3208、コピー許可3209等の項目の内容が含まれる。ここで、曲名3202、演奏者3203は、表示部3104に表示して、ユーザがコピー（複製）をするか否かを指示する判断資料となるものである。曲名コード3204は、音楽データを他の音楽データと識別するための識別子であり、曲ごとにユニークなものであり、例えばISRC (International Standard Recording Code) が付される。なお、このコードは国コード（2つのASCII文字）、オーナーコード（3つのASCII文字）、記録年（数字2桁）、シリアル番号（数字5桁）で構成されている。

【0079】記録料金3205、1回あたり再生料金3206、再生可能回数3207等は、課金基準データを構成し、いずれもその音楽データの利用料金を算定する為の情報である。記録料金3205は、通信部3101で受信されたデジタルデータを記録媒体3102に記録する際の料金である。1回あたりの再生料金3206は、記録媒体3102に記録されたデジタルデータの再生1回あたりの料金を示している。再生可能回数3207は、記録媒体3102に記録されたデジタルデータの再生が許容される回数を示している。「100回」と記録されているときには、100回に限り再生できることを示している。また、再生回数が一定回数以上になると、その後の料金が不要となる買い取り形式の設定も可能である。

【0080】暗号状態3208は、暗号有無フラグであり、通信部3101で受信されたデジタルデータが暗号化されているか否かを示すものである。コピー許可3209は、記録許可フラグであり、ユーザ側で記録する、即ち、記録媒体3102に受信された音楽データを記録することを許可するか否かを示す情報である。「1回のみ可」とは、1度だけ記録することが許可され、「許可」は、何度でも記録することが許可されていることを示している。

【0081】なお、本発明は、受信された音楽データを

記録媒体3102に記録（複製）し、再生するときの音楽の著作権保護を図ることを主目的としたものである。この音楽データをリアルタイムに聴取するだけが許可されている場合についての説明は、簡単にする。この場合は、コピー許可3209は、「不可」とされている。このデジタルデータ記録装置には、復号化部と出力部とがその構成から省略されているけれども、通信部3101で受信されたデジタルデータは復号化部で復号され、出力部から音楽が出力される。この際、課金基準データには、聴取料金が含まれている。

【0082】記録媒体3102は、書き換え可能な記憶部材からなり、装置本体に着脱可能に取り付けられており、例えば、DVD-RAM等で構成される。記録媒体3102の書き換え不能なセキュアな領域には、記録媒体3102の固有情報が予め記録されている。また、記録媒体3102には、記録部3108によって、暗号化部3107で暗号化されたデジタルデータが記録される。

【0083】更に、記録媒体3102には、記録されたデジタルデータの管理情報と属性情報とが記録部3108によって記録されている。受信データ記録判定部3103は、通信部3101からデジタルデータとその属性情報3201との通知を受けると、その属性情報3201を最初に通知されたとき記憶し、属性情報のうち、曲名3202、演奏者3203、記録料金3205、1回あたり再生料金3206等を表示部3104に表示させ、デジタルデータを暗号化部3107に通知する。

【0084】入力操作部3105からコピー（複製）指示を受けると、指示された音楽の曲名コード3204のデジタルデータのコピーが可能か否かを属性情報3201のコピー許可3209を見て判断する。コピーが許可であれば、記録媒体固有情報取得部3106に記録媒体3102の固有情報を取得するよう指示する。また、暗号化部3107に曲名コード3204と暗号状態3208を通知する。

【0085】コピーが不可であれば、表示部3104にその旨を表示させる。受信データ記録判定部3103は、記録部3108からコピー終了の通知を受けると、記憶している属性情報3201の項目、コピー許可3209を書き換える。即ち、コピー許可3209が「1回のみ」とされているときには「コピー不可」に、「何回のみ可」と数字が記録されているときには「1」を減じた数字にそれぞれ書き換える。なお、この属性情報3201を記憶する記憶領域は、EEPROM内に設けられており、このデジタルデータ記録装置の電源がオフされた場合でも記憶内容は消失されない。

【0086】例えば、暗号化部3107に曲名コード3204の「song01」を通知した後に、記録部3108からコピー終了の通知を受けると、「song01」に対応する項目、コピー許可3209を「1回のみ可」から「コピ

10

20

30

40

50

「不可」に書き換える。このようにすることによってデータ提供者の有する権利が侵されることを防止できる。

【0087】表示部3104は、液晶ディスプレイやCRT等からなり、受信データ記録判定部3103の制御により、デジタルデータである音楽データの曲名等の表示や、コピーができない旨の表示をする。入力操作部3105は、マウス等からなり、ユーザのコピー指示を受け付け、受信データ記録判定部3103に通知する。ユーザは、表示部3104に表示された曲名や演奏者の表示を見て、記録媒体3102にその音楽をダウンロードしようとするとき、マウスでその曲名等をクリックして、その音楽のコピーを指示する。

【0088】記録媒体固有情報取得部3106は、受信データ記録判定部3103から固有情報の取得指示を受けると、記録媒体3102のセキュアな領域に記録されている固有情報を読み出し、暗号化部3107に通知する。暗号化部3107は、記録媒体固有情報取得部3106から通知された固有情報を基に暗号鍵を作成する。受信データ記録判定部3103から通知されたデジタルデータを作成した暗号鍵を用いて暗号化したデジタルデータを作成し、記録部3108に通知する。

【0089】なお、受信データ記録判定部3103から通知されたデジタルデータが暗号化されている旨の通知を受けている場合には、そのデジタルデータを復号化しておいてもよいし、そのままの状態でもよい。例えば、記録媒体3102に記録すべきデジタルデータdataAを受信データ記録判定部3103から通知された場合に、記録媒体3102の固有情報を基に暗号鍵KMを作成すると、暗号化したデジタルデータE(KM, dataA)を作成する。他の記録媒体にデジタルデータdataAを記録する場合には、その他の記録媒体の固有情報を基に暗号鍵K'Mを作成したときは、暗号化したデジタルデータEは、E(K'M, dataA)となる。

【0090】ここで、デジタルデータの暗号化の技術については、特開平5-257816号公報に記載されている。記録部3108は、暗号化部3107から通知された暗号化されたデジタルデータを記録媒体3102に記録する。この際、記録媒体3102に記録したデジタルデータの管理情報を作成して、記録媒体3102に記録する。

【0091】図18は、管理情報の一例を示す図である。管理情報3301には、記録したデジタルデータの識別子である曲名コード3204と、記録媒体3102に記録されたデジタルデータの記録開始アドレス3302、記録終了アドレス3303とが対応して記録される。記録媒体3102に記録されたデジタルデータを再生する際、この管理情報3301が参照される。

【0092】また、記録部3108は、記録媒体3102に暗号化されたデジタルデータ及び管理情報の記録が終了すると、受信データ記録判定部3103に記憶さ

れている記録したデジタルデータに対応する属性情報3201を読み出し、記録媒体3102に書き込む。更に、受信データ記録判定部3103にコピー終了の通知をする。また、課金情報記録部3109に、記録したデジタルデータの曲名コードを通知する。

【0093】課金情報記録部3109は、記録部3108から曲名コード3204の通知を受けると、受信データ記録判定部3103に記憶されている曲名コード3204に対応する属性情報3201の記録料金3205を読み出し、記録料金が有料のときは、課金情報記録媒体3110にその曲名コードと記録料金と記録日時等を課金情報として記録する。

【0094】課金情報記録媒体3110は、RAMカード等からなり、記録媒体3102にダウンロードしたデジタルデータの課金情報が課金情報記録部3109によって記録される。課金部3111は、通信部3101を介して課金センタ（図示せず）からの利用料の問い合わせがあると、課金情報記録媒体3110に記録されている未決済の課金情報を読み出し、通信部3101に通知する。通知が終了すると、課金センタに通知済（決済）のフラグを課金情報記録媒体3110に記録する。

【0095】次に、本実施の形態の動作を図19のフローチャートを用いて説明する。まず、受信データ記録判定部3103は、ユーザからデジタルデータの記録指示を待ち（S3402）、指示されたデジタルデータのコピーが許可されているか否かを属性情報201を見て判断する（S3404）。否のときは、コピーが許可されていない旨を表示部3104に表示させ（S3406）、処理を終了する。

【0096】コピーが許可されているときは、記録媒体固有情報取得部3106は、記録媒体3102のセキュアな領域に記録されている記録媒体3102の固有情報を取得し、暗号化部3107に通知する（S3408）。暗号化部3107は、固有情報を基に暗号鍵を作成し、デジタルデータを暗号化する（S3410）。

【0097】記録部3108は、暗号化されたデジタルデータを記録媒体3102に記録する（S3412）。次に、課金情報記録部3109は、記録されたデジタルデータの記録料金が有料か否かを判断する（S3414）。無料であれば、処理を終了し、有料であれば、課金情報記録媒体3110に課金情報を記録して（S3416）、処理を終了する。

【0098】図20は、上述のデジタルデータ記録装置で記録媒体3102に記録されたデジタルデータの再生装置の構成図である。このデジタルデータ再生装置は、記録媒体3102と、入力操作部3501と、再生情報読出部3502と、表示部3503と、記録媒体固有情報取得部3504と、復号化部3505と、再生部3506と、課金情報記録部3507と、課金情報記録媒体3508とを備えている。

25

【0099】記録媒体3102は、上記デジタルデータ記録装置で暗号化されたデジタルデータと管理情報3301と属性情報3201とが記録されたDVD-RAMを識別する識別子である固有情報が記録されている。入力操作部3501は、ユーザから再生開始の指示を受けると、再生情報読出部3502に初期起動の指示を与える。ユーザから曲名の指示を受けると、その曲名を再生情報読出部3502に通知する。なお、初期起動の指示の他に記録媒体3102がこのデジタルデータ再生装置に挿入されたときにも自動再生モードの指示が再生情報読出部3502に与えられる。

【0100】再生情報読出部3502は、入力操作部3501から初期起動の指示を受けると、記録媒体3102に記録されている属性情報3201を読み出し、その項目である曲名3202及び演奏者3203の一覧を表示部3503に表示させる。また、入力操作部3501から曲名の指示又は、自動再生モードの指示を受けると、属性情報3201の対応する再生可能回数3207が「1」以上であるか否かを判断する。再生可能回数3207が「1」以上であれば、その曲名コード3204を読み出し、管理情報3301の記録開始アドレスから記録終了アドレスまでに記録された暗号化されたデジタルデータを読み出し、復号化部3505に通知する。この際、記録媒体固有情報取得部3504に固有情報を取得するよう指示するとともに、課金情報記録部3507に、曲名コード3204と1回あたりの再生料金3206とを通知する。更にデジタルデータの読み出しが終了すると、属性情報3201の項目である再生可能回数3207の数を「1」減じた数に書き換える。なお、再生可能回数3207が「無限」の場合には、そのままにする。

【0101】再生情報読出部3502は、再生可能回数が「1」未満であると判断したとき、表示部3503に再生可能回数が越えた旨を表示させる。表示部3503は、液晶ディスプレイ等からなり、再生情報読出部3502で読み出された曲名等を一覧表示する。また、再生可能回数を越えてのユーザからの曲名指定に対して、再生可能回数が越えた旨を表示する。

【0102】記録媒体固有情報取得部3504は、再生情報読出部3502から固有情報の取得を指示されると、記録媒体3102のセキュアな領域から記録媒体3102の識別子である固有情報を取得し、復号化部3505に通知する。復号化部3505は、記録媒体固有情報取得部3504から固有情報の通知と、再生情報読出部3502から暗号化されたデジタルデータの通知とを受けると、固有情報を基に復号鍵を作成して、暗号化されたデジタルデータを復号し、復号化したデジタルデータを再生部3506に通知する。

【0103】再生部3506は、復号化部3505からデジタルデータの通知を受けると、デコードして音楽

を再生する。音楽の再生を終了すると課金情報記録部3507に再生終了を通知する。課金情報記録部3507は、再生部3506から再生終了の通知を受けると、再生情報読出部3502から通知されている曲名コード3204と1回あたりの再生料金3206と再生日時とを課金情報として課金情報記録媒体3508に記録する。なお、1回あたりの再生料金3206が有料でなければ、記録はしない。

【0104】課金情報記録媒体3508は、RAMカード等からなり、課金情報を課金情報記録部3507によって記録される。次に、このデジタルデータ再生装置の動作を図21に示すフローチャートを用いて説明する。まず、ユーザは、再生開始を入力操作部3501のリモコン等を用いて指示し、表示部3503に表示された曲名を指定する。再生情報読出部3502は、音楽の再生要求であるとし(S3602)、指定された曲名の再生可能回数が「1」以上であるか否かを属性情報3201をみて判断する(S3604)。再生可能回数が「1」未満であれば、表示部3503に再生可能回数を超えた旨を表示させ(S3606)、処理を終了する。

【0105】再生可能回数が「1」以上の場合には、再生情報読出部3502は、記録媒体3102から暗号化されたデジタルデータを読み出し、復号化部3505に通知する(S3608)。記録媒体固有情報取得部3504は、記録媒体3102から固有情報を取得して復号化部3505に通知する(S3610)。

【0106】復号化部3505は、固有情報を復号鍵として暗号化されたデジタルデータを復号化する(S3612)。再生部3506は、デジタルデータをデコードして音楽を再生出力する(S3614)。課金情報記録部3507は、再生料金が有料であるか否かを判断し(S3616)、無料のときは何もせずに、有料のときは、課金情報を課金情報記録媒体3508に記録して(S3618)、処理を終了する。

【0107】(実施の形態7)図22は、本発明に係るデジタルデータ記録装置の実施の形態7の構成図である。このデジタルデータ記録装置は、第1デジタルデータ記録装置3700と第2デジタルデータ記録再生装置3710とからなる。第1デジタルデータ記録装置3700は、第1記録媒体3701と、通信部3101と、受信データ1次記録判定部3702と、表示部3104と、入力操作部3105と、1次記録部3703と、受信データ読出判定部3704と、固有情報取得部3705と、暗号化部3706と、課金情報記録部3109と、課金情報記録媒体3110と、課金部3111とを備えており、PCで実現される。

【0108】第2デジタルデータ記録再生装置3710は、固有情報取得送出处3707と、2次記録部3708と、第2記録媒体3709と、入力操作部3501と、再生情報読出部3502と、表示部3503と、復

号化部 3505 と、再生部 3506 と、課金情報記録部 3507 と、課金情報記録媒体 3508 とを備えている。

【0109】なお、上記実施の形態 6 のデジタルデータ記録装置及びデジタルデータ再生装置の各構成部分と同一の部分には同一の符号を付して、その説明を省略し、本実施の形態固有の部分についてのみ説明する。先ず、第 1 デジタルデータ記録装置 3700 について説明する。上記実施の形態 6 のデジタルデータ記録装置と異なるのは、第 1 記録媒体 3701 が本装置に固定的に設けられ、この第 1 記録媒体 3701 に記録されたデジタルデータが 2 次記録のために暗号化されて出力されることである。

【0110】第 1 記録媒体 3701 は、本装置 3700 内に固定的に設けられたハードディスク等の書き込み可能な記録部材からなる。第 1 記録媒体 3701 には、通信部 3101 で受信された音楽データであるデジタルデータとその管理情報とが 1 次記録部 3703 によって書き込まれる。受信データ 1 次記録判定部 3702 は、通信部 3101 で受信されたデジタルデータに付された属性データを EEPROM 内に設けられた記憶領域に書き込む。本実施の形態で受信される属性情報の一例を図 23 に示す。属性情報 3801 は、上記実施の形態 6 の属性情報 3201 と 2 次記録料金 3802 が記録されていることと、コピー許可（1 次）3803 と（2 次）3804 との記録の許可回数が表示されていることが異なる。

【0111】また、曲名コード「song05」の「曲 E」では、コピーが 1 次、2 次ともに不許可であり、リアルタイムの聴取のみが許可された音楽であることを示している。受信データ 1 次記録判定部 3702 は、ユーザからある音楽の 2 次記録の指示を受けると、先ず 1 次記録が許可されているか否かを属性情報 3801 の項目コピー許可（1 次）3803 を見て判断する。許可されていないときは、表示部 3104 に不許可である旨を表示させる。許可されているときは、指示された音楽のデジタルデータを 1 次記録部 3703 に通知する。他の機能は、上記実施の形態 6 の受信データ記録判定部 3103 と同様である。

【0112】1 次記録部 3703 は、通知されたデジタルデータを第 1 記録媒体 3701 に記録する。この際、管理情報を書き込むのは、上記実施の形態 6 の記録部 3108 と同様である。なお、上記実施の形態 6 では、記録媒体 3102 の固有情報を基に暗号鍵が作成され、デジタルデータが暗号化されていたけれども、本実施の形態では、第 1 記録媒体 3701 が取外され、他の装置で利用されることがないので暗号化されない。

【0113】また、1 次記録部 3703 は、第 1 記録媒体 3701 へのデジタルデータの記録が終了すると、受信データ読出判定部 3704 に記録した曲名コード 3

805 を通知する。受信データ読出判定部 3704 は、1 次記録部 3703 から曲名コード 3805 の通知を受けると、その音楽の 2 次記録が許可されているか否かを、受信データ 1 次記録判定部 3702 の属性情報 3801 中のコピー許可（2 次）3804 を見て判断する。許可されていないとき、又は、許可回数が「1」以上でないときには、表示部 3104 に 2 次記録が許可されていない旨を表示させる。

【0114】受信データ読出判定部 3704 は、2 次記録が許可されているときには、管理情報（図 18 参照）を見て、第 1 記録媒体 3701 に記録されている通知された曲名コードのデジタルデータを読み出して暗号化部 3706 に通知するとともに、固有情報取得部 3705 に固有情報を取得するよう指示する。また、受信データ読出判定部 3704 は、デジタルデータの読み出しが完了すると、受信データ 1 次記録判定部 3702 に記憶されている属性情報 3801 のコピー許可（2 次）3804 の回数から「1」減じた数に書き換える。例えば「1 回のみ可」であれば「不許可」に書き換え、「許可」だけであれば、回数に制限がないので、そのまま書き換えは行わない。

【0115】なお、受信データ読出判定部 3704 は、暗号化部 3706 にデジタルデータの通知の後に、受信データ 1 次記録判定部 3702 に記憶されている属性情報を読み出して通知する。固有情報取得部 3705 は、受信データ読出判定部 3704 から固有情報を取得するよう指示されると、第 1 デジタルデータ記録再生装置 3700 に接続されている第 2 デジタルデータ記録再生装置 3710 の固有情報取得送出部 3707 に、固有情報の送出を要求する。固有情報取得送出部 3707 から固有情報の通知を受けると、暗号化部 3706 に固有情報を通知する。

【0116】暗号化部 3706 は、固有情報取得部 3705 から通知された固有情報を基に暗号鍵を作成し、受信データ読出判定部 3704 から通知されたデジタルデータを暗号化して第 2 デジタルデータ記録再生装置 3710 の 2 次記録部 3708 に送出する。この暗号化されたデジタルデータの送出の後に、通知された属性情報も送出する。

【0117】次に、第 2 デジタルデータ記録再生装置 3710 について説明する。この第 2 デジタルデータ記録再生装置 3710 は、携帯型の例えばヘッドホンステレオタイプの装置で実現される。また、第 2 記録媒体 3709 がこの装置 3710 から着脱自在の半導体メモリの IC カード等から構成されている。固有情報取得送出部 3707 は、第 1 デジタルデータ記録装置 3700 の固有情報取得部 3705 から固有情報の送出要求を受けると、第 2 記録媒体 3709 に予め記録されている第 2 記録媒体固有の媒体識別情報と、この装置 3710 固有の機器識別情報とを取得して、固有情報取得部 3

705に通知する。また、再生情報読出部3502から固有情報の通知指示を受けると、復号化部3505に媒体識別情報と機器識別情報とを通知する。

【0118】2次記録部3708は、第1デジタルデータ記録装置3700の暗号化部3706から暗号化されたデジタルデータと、属性情報との出力を受けると、第2記録媒体3709に記録する。併せて、図18に示したような管理情報3301を記録する。復号化部3505は、固有情報取得送部3707から通知された媒体識別情報と機器識別情報との2つの情報を基に復号鍵を作成して、再生情報読出部3502から通知された暗号化されたデジタルデータを復号する。なお、その他の構成は、上記実施の形態6のデジタルデータ再生装置の構成とほぼ同様である。

【0119】次に、第2記録媒体3709がこの装置3710に固定的に設けられたICカード等から構成される場合について述べる。この場合には、第2記録媒体3709がこの装置3710以外で再生されることがないことから固有情報取得送部3707は、媒体識別情報を取得することなく、自ら記憶している機器識別情報を固有情報取得部3705に通知する。また、復号化部3505にも、機器識別情報を通知する。

【0120】このように、第2デジタルデータ記録再生装置3710に設けられた第2記録媒体3709が着脱自在であるか否かによって、デジタルデータの暗号化の暗号鍵の作成を媒体識別情報と機器識別情報との組合せによるか、機器識別情報だけで行うかを使い分けることができる。このように使い分けることによって、デジタルデータの不正な複製や不正な再生利用を防止することができる。

【0121】次に、本実施の形態の動作を図24に示すフローチャートを用いて説明する。まず、受信データ1次記録判定部3702は、入力操作部3105からデジタルデータの2次記録の指示が有るのを待ち(S3902)、デジタルデータの1次記録が許可されているか否かを属性情報3801を見て判断する(S3904)。許可されていないときは、その旨を表示部3104に表示させて(S3906)、処理を終了する。

【0122】許可されているときは、受信データ1次記録判定部3702は、デジタルデータを1次記録部3703に通知する。1次記録部3703は、第1記録媒体3701にデジタルデータと管理情報とを記録する(S3908)。次に、課金情報記録部3109は、1次記録に対して課金されているか否かを判断し(S3910)、1次コピーが有料の時は課金情報を課金情報記録媒体3110に記録する(S3912)。

【0123】次に、受信データ読出判定部3704は、第1記録媒体3701に記録されたデジタルデータの2次記録が許可されているか否かを受信データ1次記録判定部3702に記憶されている属性情報3801を見

て判断する(S3914)。許可されていないときは、2次記録が許可されていない旨を表示部3104に表示させ(S3916)、処理を終了する。

【0124】許可されているときは、受信データ読出判定部3704は、第1記録媒体3701からデジタルデータを読み出し、暗号化部3706に通知するとともに、固有情報取得部3705に第2デジタルデータ記録再生装置3710から固有情報を取得するよう指示する。固有情報取得部3705は、固有情報を取得し、暗号化部3706に通知する(S3918)。暗号化部3706は、通知された固有情報を基に暗号鍵を作成し(S3920)、通知されているデジタルデータを暗号化して第2デジタルデータ記録再生装置3710の2次記録部3708に出力する。

【0125】2次記録部3708は、通知された暗号化されたデジタルデータと属性情報と管理情報とを第2記録媒体3709に記録する(S3922)。また、課金情報記録部3109は、2次記録に対して課金されているか否かを判断し(S3924)、2次記録が有料のときは、課金情報を課金情報記録媒体110に記録し(S3926)、処理を終了する。

【0126】なお、第2デジタルデータ記録再生装置3710でのデジタルデータの再生動作は、実施の形態6のデジタルデータ再生装置の動作とほぼ同様であるので説明を省略する。

(変形例) 上記実施の形態7では、第2記録媒体3709が着脱自在であるときには、第2デジタル記録再生装置3710の機器識別情報と、第2記録媒体3709の媒体識別情報とを組合せた暗号鍵でデジタルデータが暗号化されたけれども、本変形例では、暗号化の形態(媒体識別情報のみに基づいた暗号鍵とするのか媒体識別情報に機器識別情報を組合せた暗号鍵とするのか)をユーザに指定させ、ユーザの利用形態の自由度を拡大している。即ち、第2デジタルデータ記録再生装置3710で第2記録媒体3709に記録された音楽を再生しようとするときには、媒体識別情報及び機器識別情報でデジタルデータを暗号化して記録するようにし、他のデジタルデータ再生装置(媒体識別情報を復号鍵として暗号化されたデジタルデータを復号化できる装置)で第2記録媒体3709に記録された音楽を再生しようとするときには、媒体識別情報でデジタルデータを暗号化して記録するようにする。ユーザの利用形態に応じて暗号化の形態を選択できるようにしている。

【0127】一方、このユーザの利用の自由度に応じて2次記録料金を設定して、著作権の保護を図っている。以下、本変形例の具体的構成を説明する。なお、本変形例は、図22に示した第1デジタルデータ記録装置3700の構成に若干の機能を追加するものであるので、実施の形態7の構成図をそのまま利用して、本変形例固有の構成についてのみ説明する。

・【0128】図25は、受信データ1次記録判定部3702に記憶されている属性情報31001の一部を示している。この属性情報31001では、図23に示した属性情報3801の2次記録料金3802と2次記録料金31002との内容が異なる。2次記録料金31002は、暗号化の暗号鍵が媒体識別情報（媒体ID）31003、機器識別情報（機器ID）31004、媒体識別情報と機器識別情報との組み合わせ31005のいずれであるかによって異なっている。媒体識別情報31003を基に暗号鍵が作成されたものでは、他の装置に第2記録媒体3709を装着して音楽を再生でき、ユーザの自由度が増すことから2次記録料金（2次複製利用料金）が機器識別情報31004又は媒体識別情報と機器識別情報との組み合わせ31005を基に暗号鍵が作成されたものよりも高額に設定される。ユーザの利用形態の拡大に応じて複製利用料金を課金できるようにしたものである。

【0129】固有情報取得部3705は、固有情報取得送出部3707から機器識別情報と媒体識別情報との通知を受けると、表示部3104に第2記録媒体3709を他の装置で利用するか、第2デジタルデータ記録再生装置3710でのみ利用するかを表示させ、ユーザの選択を待つ。ユーザは、入力操作部3105より、他の装置を用いるか、第2デジタルデータ記録再生装置3710のみを用いるかを指定する。即ち、暗号鍵を媒体識別情報だけで作成するか、媒体識別情報と機器識別情報との組み合わせで作成するかを指示する。

【0130】入力操作部3105は、この指定を固有情報取得部3705と受信データ1次記録判定部3702とに通知する。受信データ1次記録判定部3702は、入力操作部3105から他の装置を用いるとの通知を受けると、課金情報記録部3109に媒体識別情報31003を暗号鍵とする2次記録料金である旨を、第2デジタルデータ記録再生装置のみを用いるとの通知を受けると、媒体識別情報と機器識別情報との組み合わせ31005を暗号鍵とする2次記録料金である旨を通知する。

【0131】固有情報取得部3705は、入力操作部3105から、他の装置を用いる旨の通知を受けると、暗号化部3706に媒体識別情報のみを通知する。また、第2デジタルデータ記録再生装置3710でのみ用いる旨の通知を受けると、同様に媒体識別情報と機器識別情報とを通知する。課金情報記録部3109は、暗号化部3706から暗号化されたデジタルデータを2次記録部3708に送出した旨の通知を受けると、受信データ1次記録判定部3702から通知されている属性情報31001の2次記録料金31002を見て、課金情報記録媒体3110に課金情報を記録する。

【0132】なお、本変形例において、第2記録媒体が着脱自在のDVD-RAMであるときには、上記実施の形態6と同様、DVD-RAM固有の識別情報のみを基に暗号鍵を作

成し、デジタルデータを暗号化して記録するようにできるのは勿論である。また、本変形例の動作は、上記実施の形態7の動作と基本的に異なるところがないのでその説明は省略する。

【0133】なお、上記実施の形態6、7及び変形例において、課金情報記録媒体3110、3508は例えばICカードにより実現し、デジタルデータの記録や再生時にICカードをセットしなければ動作しないとしても可能である。また、上記実施の形態6、7及び変形例では、通信部3110で受信されるデジタルデータが音楽データであるとして説明したけれども、これに限ることはなく、映像データ、音声データ、文字データやこれらの組合せであってもよいのは勿論である。

【0134】上記実施の形態6と実施の形態7と変形例のデジタルデータ記録装置及び再生装置並びにデジタルデータ記録再生装置は、図16、図20及び図22にその構成図を示したけれども、各構成要素の機能を発揮するプログラムをコンピュータ読取可能なフロッピーディスク等の記録媒体に記録しておき、著作権の保護機能を有しないデジタルデータ記録再生装置に適用して著作権の保護機能を有する装置とすることができる。

【0135】

【発明の効果】以上説明したように、本発明は、デジタルデータを記録媒体に記録するデジタルデータ記録装置において、暗号化されたデジタルデータをデジタルネットワークを介して受信する通信手段と、前記通信手段により受信された暗号化デジタルデータを復号する復号化手段と、複数の暗号化部を有し、当該暗号化部はそれぞれ異なるセキュリティレベルを有する暗号化方式の一つでデジタルデータを暗号化する暗号化手段と、前記暗号化手段により暗号化されたデジタルデータを前記記録媒体に記録する記録手段と、前記復号化手段と前記暗号化手段とを制御する制御手段とを備え、前記制御手段は、前記複数の暗号化部の一つで、前記復号化手段により復号化されたデジタルデータを再暗号化させることとしている。

【0136】このような構成によって、再生装置で容易に再生できる暗号化部で再暗号化されたデジタルデータを記録媒体に記録することができ、かつ暗号化されているので著作権の保護を図ることができる。また、前記記録媒体に記録されたデジタルデータは、再生装置により再生され、前記暗号化手段は、前記記録媒体の識別情報を基に生成した暗号鍵によりデジタルデータを暗号化する第1暗号化部と、前記再生装置の識別情報を基に生成した暗号鍵によりデジタルデータを暗号化する第2暗号化部とを有し、前記制御手段は、前記記録媒体が再生装置から着脱可能か否かを判定し、着脱可能なときは、前記第1暗号化部によりデジタルデータの暗号化を行わせ、着脱不可能なときは、前記第2暗号化部によりデジタルデータの暗号化を行わせることとしてい

る。

【0137】このような構成によって、記録媒体がいずれかの再生装置で再生されるときには、その記録媒体の識別情報を基に生成される暗号鍵でデジタルデータを暗号化し、特定の一の再生装置で再生されるときには、その一の再生装置の識別情報を基に生成される暗号鍵でデジタルデータを暗号化することによって、記録媒体に記録されたデジタルデータを再生装置で再生することができる。

【0138】また、前記デジタルデータ記録装置は、更に、前記デジタルネットワークを介して課金処理を行う課金手段を備え、前記制御手段は、再暗号化を行う前記暗号化部の選択に基づいて課金値を決定し、決定した課金値に基づき課金処理を行うように前記課金手段を制御することとしている。このような構成によって、異なるセキュリティレベルを有する暗号化方式の暗号化部を選択することができ、かつ、暗号化部に応じた料金を支払うことができる。

【0139】また、前記制御手段は、前記暗号化手段が前記暗号鍵を生成できない場合は、受信された暗号化デジタルデータを、前記復号化手段により復号化することを禁止することとしている。このような構成によって、暗号化部で暗号鍵を生成できないときには、デジタルデータを復号する処理をなくすことができる。

【0140】また、前記暗号化手段の有する複数の暗号化部による暗号化されたデジタルデータは、前記通信手段により受信されたデジタルデータの暗号化に比べいずれもセキュリティレベルが低いこととしている。このような構成によって、再生装置は、デジタルデータの再生が容易となり、再生装置のコストダウンにつながる。

【0141】また、前記通信手段により受信されるデジタルデータは異なるセキュリティレベルを有する暗号化方式の一つで暗号化されており、前記受信されるデジタルデータは当該デジタルデータの暗号化方式を示す属性情報を含み、前記復号化手段は、複数の復号化部を含み、当該復号化部は前記異なるセキュリティレベルを有する暗号化方式で暗号化されたデジタルデータをそれぞれ復号化し、前記制御手段は、前記通信手段により受信された暗号化デジタルデータの暗号化方式を前記属性情報に基づいて判定し、判定した暗号化方式に対応する前記復号化部により前記暗号化デジタルデータを復号化するように前記復号化手段を制御することとしている。

【0142】このよな構成によって、受信されたデジタルデータごとに異なるセキュリティレベルを有する暗号化方式で暗号化されていても、暗号化方式に対応した復号化部を選んで、復号化することができる。また、前記デジタルデータ記録装置は、更に、前記デジタルネットワークを介して課金処理を行う課金手段を備え、

前記制御手段は、受信した暗号化デジタルデータに対し、復号化を行う前記復号化部の選択と再暗号化を行う前記暗号化部の選択とに基づいて課金値を決定し、決定した課金値に基づき課金処理を行うように前記課金手段を制御することとしている。

【0143】このような構成によって、デジタルデータの復号化と再暗号化とに対応した利用料金が徴収され、著作権の保護を図ることができる。また、本発明は、デジタルデータを記録媒体に記録するデジタルデータ記録方法において、暗号化されたデジタルデータをデジタルネットワークを介して受信する通信ステップと、前記通信ステップにより受信された暗号化デジタルデータを復号する復号化ステップと、複数の異なるセキュリティレベルを有する暗号化方式の一つで復号化されたデジタルデータを暗号化する暗号化ステップと、前記暗号化ステップにより暗号化されたデジタルデータを前記記録媒体に記録する記録ステップとを有することとしている。

【0144】このような構成によって、再生装置で容易に再生できる暗号化方式で暗号化されたデジタルデータを記録媒体に記録することができ、かつ、暗号化されているので著作権の保護を図ることができる。また、前記通信ステップにより受信されるデジタルデータは異なるセキュリティレベルを有する暗号化方式の一つで暗号化されており、前記受信されるデジタルデータは当該デジタルデータの暗号化方式を示す属性情報を含み、複数の暗号化方式から一の暗号化方式を前記属性情報に基づいて判定する判定ステップを更に有し、前記復号化ステップは、前記判定ステップに従い暗号化されたデジタルデータを復号化することとしている。

【0145】このような構成によって、通信手段で受信された暗号化されたデジタルデータが異なるセキュリティレベルを有する暗号化方式で暗号化されていても、復号化することができる。更に本発明は、デジタルデータを第1記録媒体に記録するデジタルデータ記録装置に適用されるコンピュータ読み取り可能な記録媒体において、暗号化されたデジタルデータをデジタルネットワークを介して受信する通信ステップと、前記通信ステップにより受信された暗号化デジタルデータを復号する復号化ステップと、複数の異なるセキュリティレベルを有する暗号化方式の一つで復号化されたデジタルデータを暗号化する暗号化ステップと、前記暗号化ステップにより暗号化されたデジタルデータを前記第1記録媒体に記録する記録ステップとの各ステップをコンピュータに実行させるプログラムを記録したコンピュータ読み取り可能な記録媒体としている。

【0146】このような構成によって、容易に再生できる暗号化方式で暗号化されたデジタルデータを記録媒体に記録し、かつ、著作権の保護を図る機能のないデジタルデータ記録装置に適用して、このような機能を発

揮させることができる。ここで、前記通信ステップにより受信されるデジタルデータは異なるセキュリティレベルを有する暗号化方式の一つで暗号化されており、前記受信されるデータは当該データの暗号化方式を示す属性情報を含み、複数の暗号化方式から一の暗号化方式を前記属性情報に基づいて判定する判定ステップを更に有し、前記復号化ステップは、前記判定ステップに従い暗号化されたデジタルデータを復号化することをコンピュータに実行させることとしている。

【0147】このような構成によって、通信手段で受信された暗号化されたデジタルデータが異なるセキュリティレベルを有する暗号化方式で暗号化されていても復号化することができる。

【図面の簡単な説明】

【図1】本発明に係るデジタルデータ記録装置の実施の形態1の構成図である。

【図2】上記実施の形態のハード構成を示す外観図及び上記実施の形態で得られた記録媒体の再生装置の外観図である。

【図3】上記実施の形態の音楽データの購入のために開設されたホームページの表示画面の一例を示す図である。

【図4】上記実施の形態の一次記録媒体にダウンロードされた音楽データのデータ構造の一例を示す図である。

【図5】上記実施の形態の音楽データの購入のために開設されたホームページの表示画面の他の一例を示す図である。

【図6】上記実施の形態の動作を説明するフローチャートのその1である。

【図7】上記実施の形態の動作を説明するフローチャートのその2である。

【図8】本発明に係るデジタルデータ記録装置の実施の形態2の構成図である。

【図9】上記実施の形態の情報提供者が提供するデジタル信号を記録する際の表示部に表示される情報を示す図である。

【図10】上記実施の形態の動作を示すフローチャートである。

【図11】本発明に係るデジタルデータ記録装置の実施の形態3の構成図である。

【図12】上記実施の形態の情報提供者が提供するデジタル信号の属性情報のデータ構造を示す図である。

【図13】上記実施の形態の動作を示すフローチャートのその1である。

【図14】上記実施の形態の動作を示すフローチャートのその2である。

【図15】本発明に係るデジタルデータ記録装置の実施の形態4の構成図である。

【図16】本発明に係るデジタルデータ記録装置の実施の形態6の構成図である。

【図17】上記実施の形態のデジタルデータに付されて送信される属性情報のデータ構造の一例を示す図である。

【図18】上記実施の形態の記録媒体に記録される管理情報のデータ構造の一例を示す図である。

【図19】上記実施の形態の動作を説明するフローチャートである。

【図20】上記実施の形態で記録された記録媒体を再生するデジタルデータ再生装置の構成図である。

【図21】上記デジタルデータ再生装置の動作を説明するフローチャートである。

【図22】本発明に係るデジタルデータ記録装置の実施の形態7の構成図である。

【図23】上記実施の形態のデジタルデータに付されて送信される属性情報のデータ構造の一例を示す図である。

【図24】上記実施の形態の動作を説明するフローチャートである。

【図25】上記実施の形態7の変形例のデジタルデータに付されて送信される属性情報のデータ構造の一例を示す図である。

【符号の説明】

100、2101	データ送受信部
101	受付部
102、2102	一次記録媒体
103、2103	データ取出部
104	判定部
105、2115	復号化部郡
106	第1復号化部
107	第2復号化部
108	第n復号化部
109	暗号方式指示部
110	暗号化部郡
111	第1暗号化部
112	第2暗号化部
113	第n暗号化部
114、2110、3709	二次記録媒体
115、2109、3108	記録部
116、2802、3705	固有情報取得部
117	指示受付部
118、3111	課金部
201	パーソナルコンピュータ
202	DVD-RAMドライブ
203	DVD-RAMディスク
204	DVD-Audioプレーヤ
2104	暗号方式判定部
2105	第1の復号化部
2106	第2の復号化部
2107	第nの復号化部
2108、3706	暗号化部

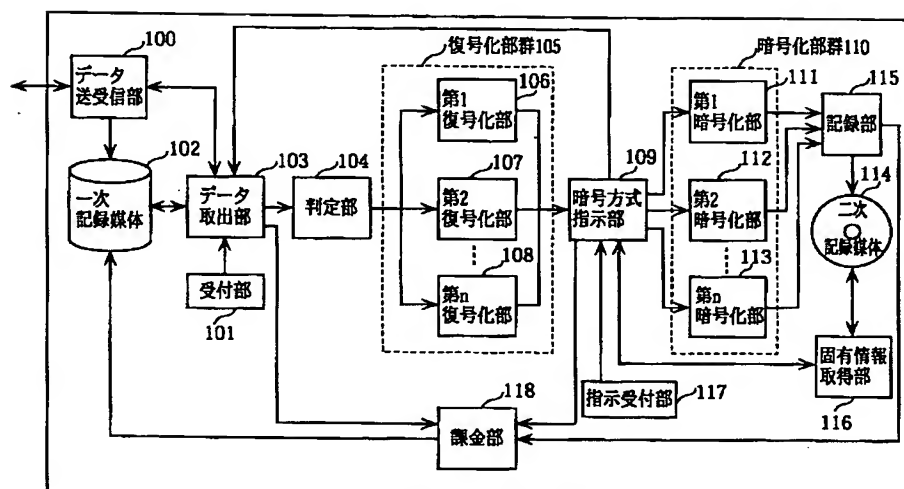
37

2111 入力部
 2112、3104 表示部
 2113 記録媒体固有情報取得部
 2401 属性情報取得部
 2402 コピー制御情報検出判定部
 2403 コピー制御情報変換部
 2404 課金情報算出部
 2800 第1のデジタルデータ記録装置
 2801 第2のデジタルデータ記録装置
 2803、3707 固有情報取得送部
 3101 通信部

38

記録媒体
 受信データ記録判定部
 入力操作部
 課金情報記録部
 課金情報記録媒体
 第1デジタルデータ記録装置
 第1記録媒体
 1次記録部
 受信データ読出判定部
 第2デジタルデータ記録再生装置

【図1】

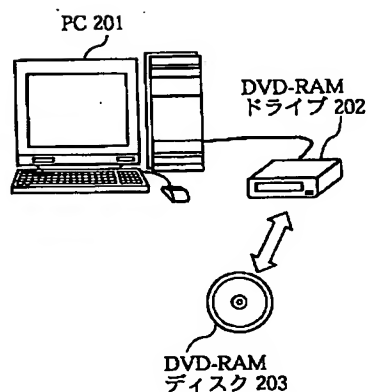


デジタルデータ記録装置

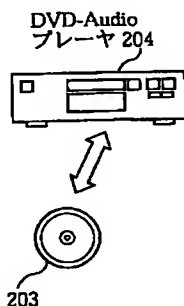
【図18】

管理情報 3301		
曲名コード	記録開始アドレス	記録終了アドレス
song01	00320	00933
song02	14902	15172
song03	13085	13994
song04	50870	51825
song05	58349	58783

【図2】

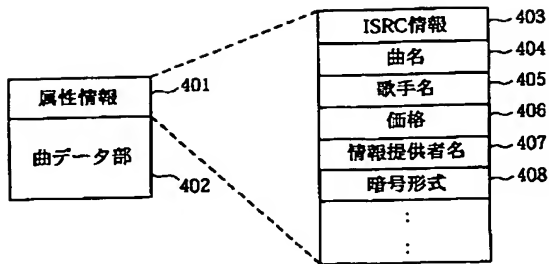


【図3】



曲名	歌手名	収録時間	価格
Song1	SingerA	4分20秒	100円
Song2	SingerB	3分53秒	50円
Song3	SingerC	4分48秒	75円
Song4	SingerD	4分06秒	100円
:	:	:	:
:	:	:	:

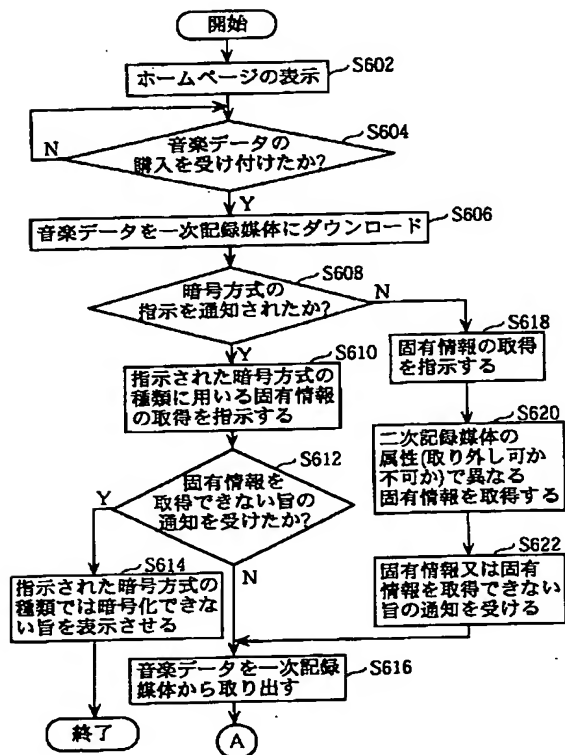
【図 4】



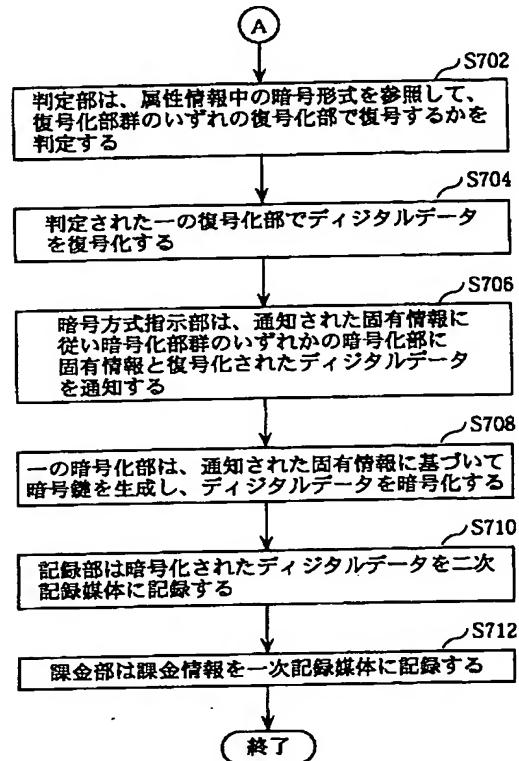
【図 5】

301	302	303	501	502
曲名	歌手名	収録時間	価格(1)	価格(2)
Song1	SingerA	4分20秒	100円	70円
Song2	SingerB	3分53秒	50円	35円
Song3	SingerC	4分48秒	75円	50円
Song4	SingerD	4分06秒	100円	100円
:	:	:	:	:
:	:	:	:	:

【図 6】



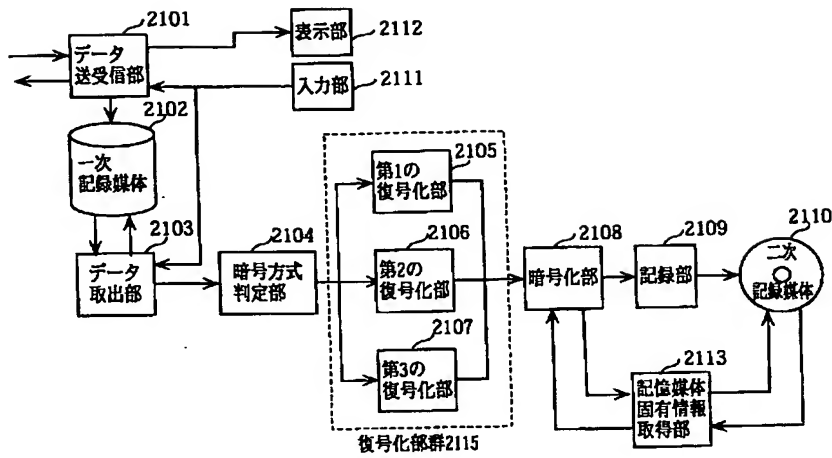
【図 7】



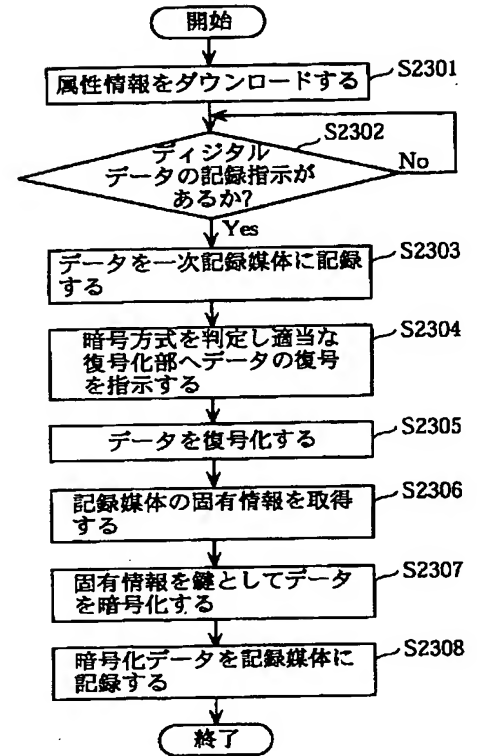
【図 9】

2201	2202	2203	2204
曲名	曲名コード	歌手名	データ入手先
曲A	song01	A	www.song/song01
曲B	song02	B	www.song/song02
曲C	song03	C	www.song/song03
曲D	song04	D	www.song/song04
曲E	song05	E	www.song/song05

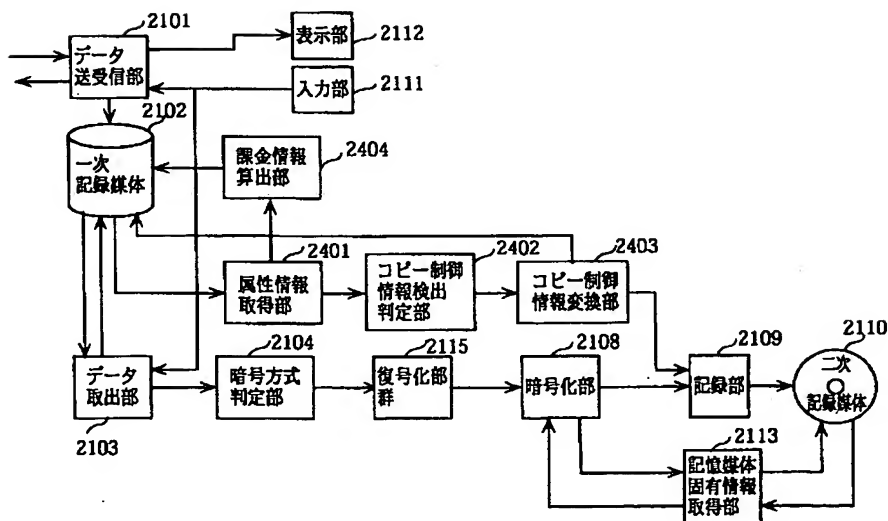
【図 8】



【図 10】



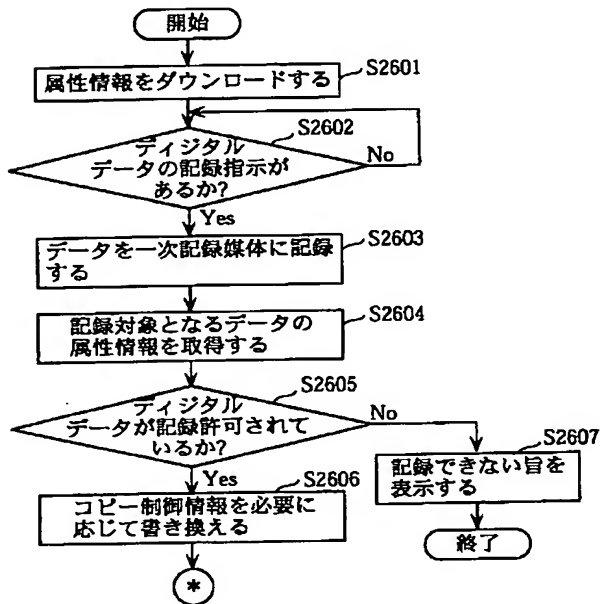
【図 11】



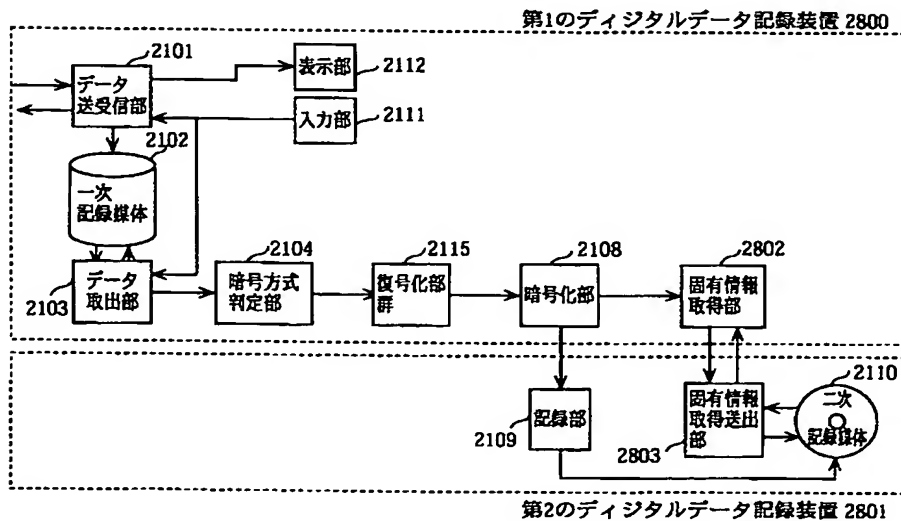
【図 1 2】

2201	2202	2203	2204	2501	2502
曲名	曲名コード	歌手名	データ入手先	コピー制御情報	価格
曲A	song01	A	www. song/song01	孫コピー不可	100円
曲B	song02	B	www. song/song02	無制限に許可	10円
曲C	song03	C	www. song/song03	孫コピー不可	0円
曲D	song04	D	www. song/song04	孫コピー不可	30円
曲E	song05	E	www. song/song05	2回コピー可	10円

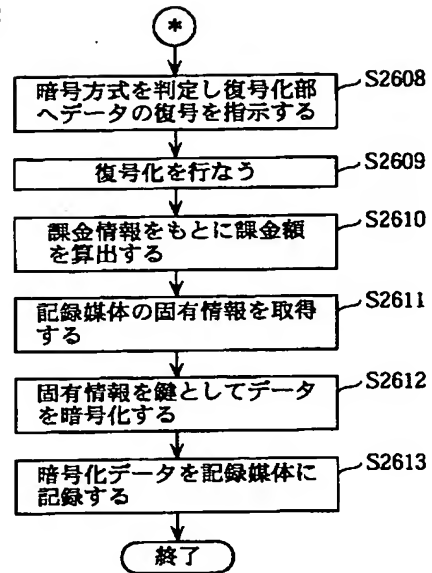
【図 1 3】



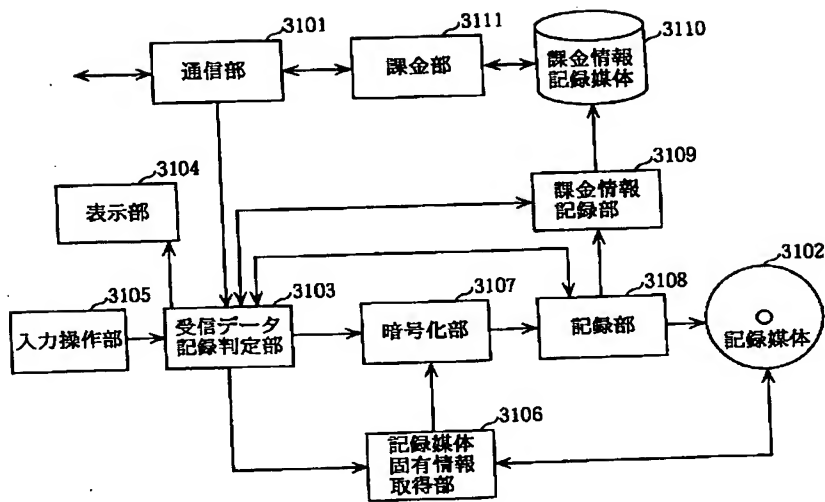
【図 1 5】



【図 1 4】



【図 16】



【図 17】

属性情報 3201

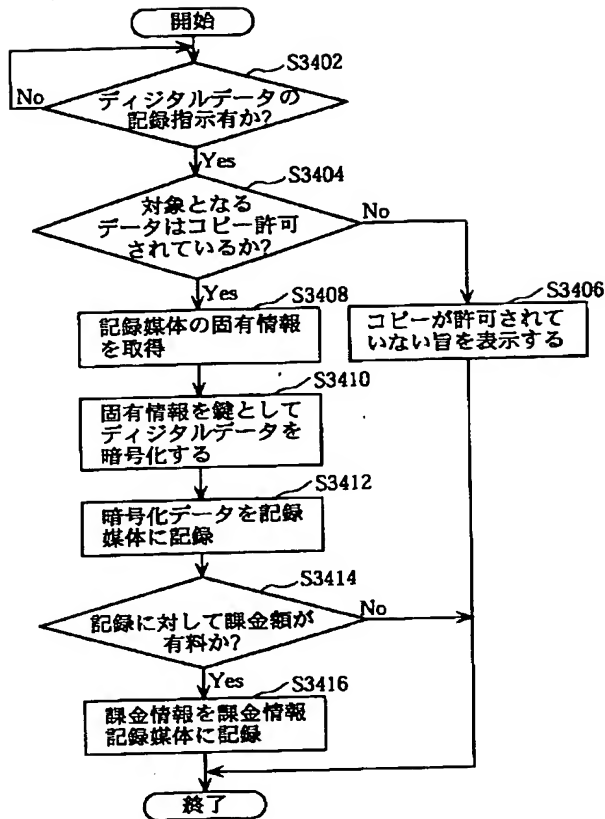
3202	3203	3204	3205	3206	3207	3208	3209	
曲名	演奏者	曲名コード	記録料金	1回あたり再生料金	再生可能回数	暗号状態	コピー許可	...
曲A	a	song01	100円	0.5円	100回	暗号あり	1回のみ可	...
曲B	b	song02	10円	0円	無限	暗号なし	許可	...
曲C	c	song03	0円	1円	50回	暗号あり	1回のみ可	...
曲D	d	song04	30円	5円	50回	暗号あり	1回のみ可	...
曲E	e	song05	10円	0円	10回	暗号なし	許可	...

【図 23】

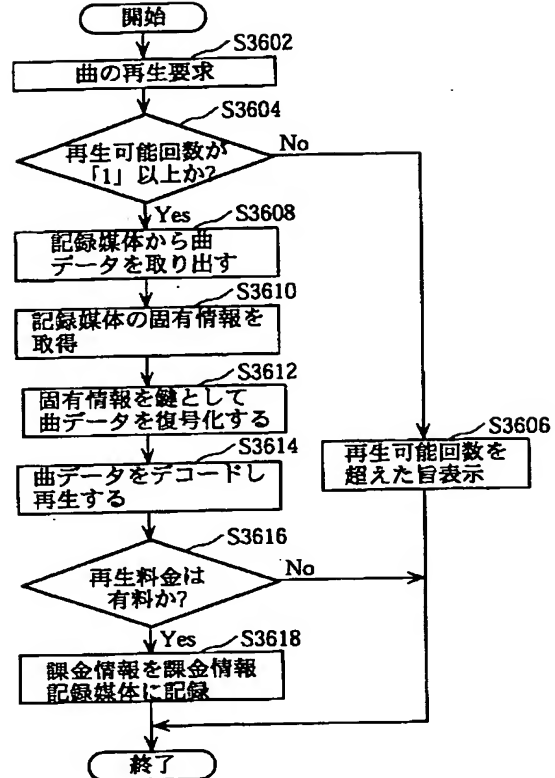
属性情報 3801

		3805	3802		3803		3804			
曲名	演奏者	曲名コード	1次記録料金	2次記録料金	1回あたり再生料金	再生可能回数	暗号状態	コピー許可(1次)	コピー許可(2次)	...
曲A	a	song01	0円	100円	0.5円	100回	暗号あり	1回のみ可	1回のみ可	...
曲B	b	song02	10円	10円	0円	無限	暗号なし	許可	許可	...
曲C	c	song03	0円	0円	1円	50回	暗号あり	1回のみ可	1回のみ可	...
曲D	d	song04	0円	30円	5円	50回	暗号あり	1回のみ可	1回のみ可	...
曲E	e	song05	—	—	—	—	暗号なし	不許可	不許可	...

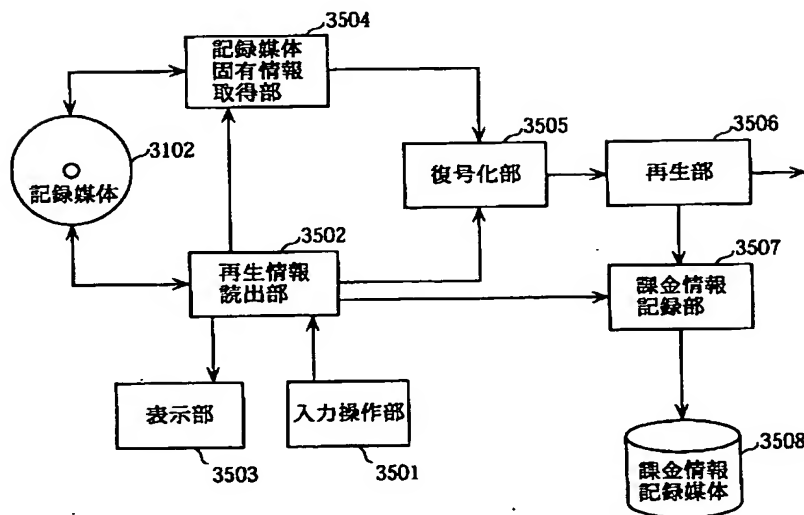
【図 19】



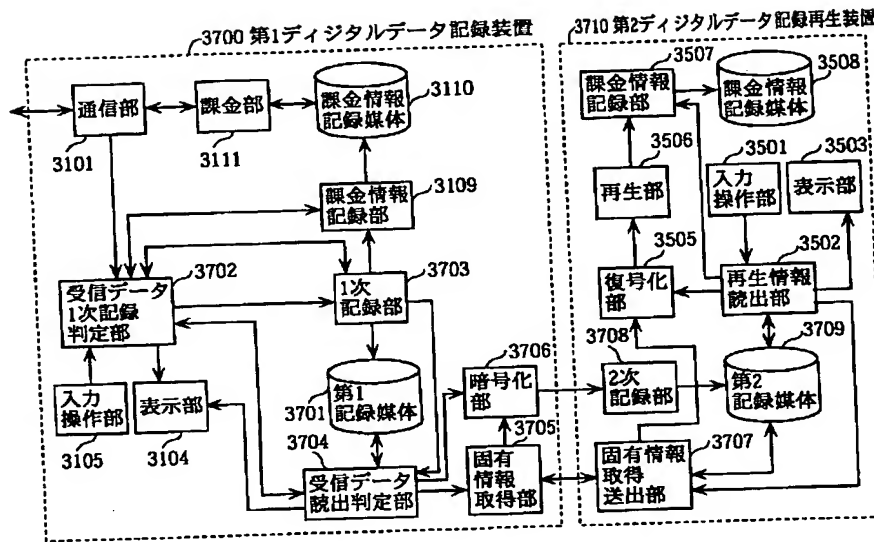
【図 21】



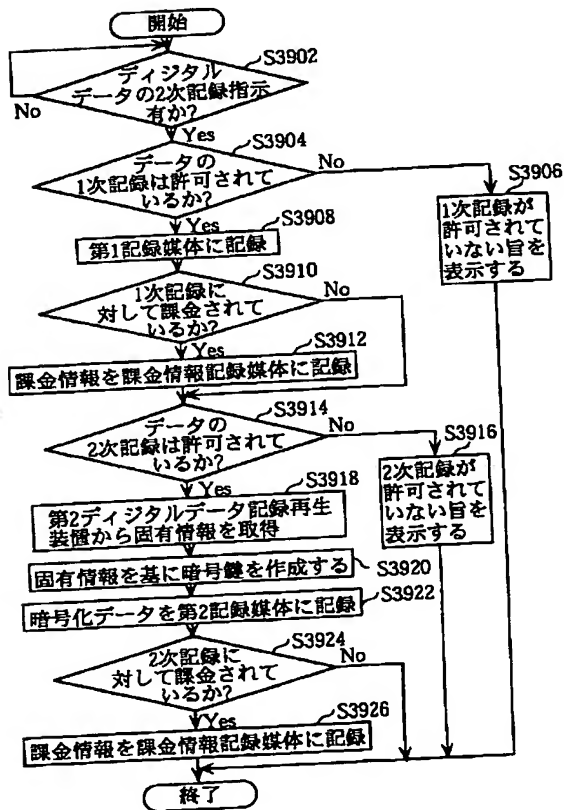
【図 20】



【図 2 2】



【図 2 4】



【図25】

属性情報31001						
			31003	31002	31004	31005
...	曲名 コード	...	2次記録料金			...
			媒体ID	機器ID	媒体ID+機器ID	
...	song01	...	100円	10円	10円	...
...	song02	...	10円	1円	1円	...
...	song03	...	0円	0円	0円	...
...	song04	...	30円	3円	3円	...
...	song05	...	10円	1円	1円	...



PCT

特許協力条約に基づいて公開された国際出願

(51) 国際特許分類6 G11B 20/10		A1	(11) 国際公開番号 WO00/05716
		(43) 国際公開日 2000年2月3日(03.02.00)	
(21) 国際出願番号 PCT/JP99/03887		(74) 代理人 中島司朗(NAKAJIMA, Shiro) 〒531-0072 大阪府大阪市北区豊崎三丁目2番1号 淀川5番館6F Osaka, (JP)	
(22) 国際出願日 1999年7月21日(21.07.99)			
(30) 優先権データ 特願平10/206967 1998年7月22日(22.07.98) JP 特願平10/289831 1998年10月12日(12.10.98) JP		(81) 指定国 AU, CN, ID, KR, MX, SG, 欧州特許 (DE, FR, GB, IT, NL)	
(71) 出願人 松下電器産業株式会社 (MATSUSHITA ELECTRIC INDUSTRIAL CO., LTD.)[JP/JP] 〒571-8501 大阪府門真市大字門真1006番地 Osaka, (JP)		添付公開書類 国際調査報告書	
(72) 発明者 田川健二(TAGAWA, Kenji) 〒576-0021 大阪府交野市妙見坂5丁目5番地305号 Osaka, (JP) 南 賢尚(MINAMI, Masataka) 〒656-2311 兵庫県津名郡東浦町久留麻2349-1 Hyogo, (JP) 小塚雅之(KOZUKA, Masayuki) 〒572-0024 大阪府寝屋川市石津南町19番1-1207号 Osaka, (JP)			
(54)Title: DIGITAL DATA RECORDING DEVICE AND METHOD FOR PROTECTING COPYRIGHT AND EASILY REPRODUCING ENCRYPTED DIGITAL DATA AND COMPUTER READABLE RECORDING MEDIUM RECORDING PROGRAM			
(54)発明の名称 著作権を保護し、記録媒体に記録された暗号化されたデジタルデータの再生を容易にするデジタルデータ記録装置及びその方法並びにそのプログラムを記録したコンピュータ読み取り可能な記録媒体			
(57) Abstract A data transmitting/receiving unit receives electronically allotted encrypted digital data for recording on a primary recording medium. Digital data use provider-dependent different encryption systems and contain attribute information describing encryption systems. Digital data retrieved at a data retrieving unit is judge for an encryption system at a judging unit and is decoded at one proper decoding unit. An inherent information acquiring unit acquires identification information of a secondary recording medium or a reproducing device depending on whether or not the second recording medium is mountable/demountable to/from the reproducing device. An encryption system instructing unit selects one encrypting unit out of a plurality of encrypting units based on the acquired identification information. The one encrypting unit creates an encryption key based on the identification information and encrypts digital data. A recording unit records digital data on the secondary recording medium, and an accounting unit charges costs according to accounting information described in the attribute information.			
		 <p>A デジタルデータ記録装置</p> <p>A ... DIGITAL DATA RECORDING DEVICE 100 ... DATA TRANSMITTING/RECEIVING UNIT 101 ... JUDGING UNIT 102 ... DECODING UNIT 103 ... ENCRYPTION SYSTEM INSTRUCTING UNIT 104 ... ENCRYPTING UNIT 105 ... RECORDING UNIT 106 ... ACCOUNTING UNIT 107 ... IDENTIFICATION INFORMATION ACQUIRING UNIT 108 ... ENCRYPTION SYSTEM INSTRUCTING UNIT 109 ... ENCRYPTING UNIT 110 ... RECORDING UNIT 111 ... ACCOUNTING UNIT 112 ... IDENTIFICATION INFORMATION ACQUIRING UNIT 113 ... ENCRYPTION SYSTEM INSTRUCTING UNIT 114 ... ENCRYPTING UNIT 115 ... RECORDING UNIT 116 ... ACCOUNTING UNIT</p>	

(57)要約

データ送受信部は、電子配信される暗号化されたデジタルデータを受信し、一次記録媒体に記録する。デジタルデータは、提供者ごとに暗号方式が異なり、暗号形式を記載した属性情報を含んでいる。データ取出部で取り出されたデジタルデータは、判定部で暗号形式が判定され、適切な一の復号化部で復号される。固有情報取得部は、二次記録媒体が再生装置に対して着脱可能か否かで二次記録媒体又は再生装置の識別情報を取得する。暗号方式指示部は、取得された識別情報に従い、複数の暗号化部から一の暗号化部を選ぶ。一の暗号化部は、識別情報を基に暗号鍵を生成し、デジタルデータを暗号化する。記録部は二次記録媒体にデジタルデータを記録し、課金部は、属性情報に記載された課金情報に従い課金する。

PCTに基づいて公開される国際出願のパンフレット第一頁に掲載されたPCT加盟国を同定するために使用されるコード(参考情報)

AE アラブ首長国連邦	DM ドミニカ	KZ カザフスタン	RU ロシア
AL アルバニア	EE エストニア	LC セントルシア	SD スーダン
AM アルメニア	ES スペイン	LI リヒテンシュタイン	SE スウェーデン
AT オーストリア	FI フィンランド	LK スリランカ	SG シンガポール
AU オーストラリア	FR フランス	LR リベリア	SI スロヴェニア
AZ アゼルバイジャン	GA ガボン	LS レソト	SK スロヴァキア
BA ボスニア・ヘルツェゴビナ	GB 英国	LT リトアニア	SL シェラ・レオネ
BB バルバドス	GD グレナダ	LU ルクセンブルグ	SN セネガル
BF ベルギー	GE グルジア	LV ラトヴィア	SZ スワジランド
BG ブルガリア	CH ガーナ	MA モロッコ	TD チャード
BH バハマ	CM ガンビア	MC モナコ	TG トーゴ
BJ ベナン	CN ギニア・ビサウ	MD モルドヴァ	TJ タジキスタン
BR ブラジル	CR キリチア	MG マダガスカル	TZ タンザニア
BY ベラルーシ	HR クロアチア	MK マケドニア旧ユーゴスラヴィア	TM トルクメニスタン
CA カナダ	HU ハンガリー		TR トルコ
CF 中央アフリカ	ID インドネシア	ML マリ	TT トリニダード・トバゴ
CG コンゴ	IE アイルランド	MN モンゴル	UA ウクライナ
CH スイス	IL イスラエル	MR モーリタニア	UG ウガンダ
CI コートジボアール	IN インド	MW マラウイ	US 米国
CM カメルーン	IS アイスランド	MX メキシコ	UZ ウズベキスタン
CN 中国	IT イタリア	NE ニジェール	VN ヴィエトナム
CR コスタ・リカ	JP 日本	NL ノールウェー	YU ユーゴスラビア
CU キューバ	KE ケニア	NO ノールウェー	ZA 南アフリカ共和国
CY キプロス	KG キルギスタン	NZ ニュージーランド	ZW ジンバブエ
CZ チェッコ	KP 北朝鮮	PL ポーランド	
DE ドイツ	KR 韓国	PT ポルトガル	
DK デンマーク		RO ルーマニア	

明 細 書

著作権を保護し、記録媒体に記録された暗号化されたデジタルデータの再生を容易にするデジタルデータ記録装置及びその方法並びにそのプログラムを記

5 録したコンピュータ読み取り可能な記録媒体

技術分野

本発明は、デジタルデータの著作権保護を図るデジタルデータ記録装置及びその方法並びにコンピュータ読み取り可能な記録媒体に関する。

10

背景技術

近年のインターネットの普及により、PC（パーソナルコンピュータ）を用いて、ホームページ上から好みの音楽データなどをダウンロードにより入手し、クレジットカードなどの決済手段を通じて支払いを行う、いわゆる EC(Electronic Commerce：電子商取引)による音楽流通が広がりつつある。このようなインターネットを通じた EC による音楽流通（以下「電子音楽配信」という。）が普及することは、ユーザがレコード店に行く必要がなくなることを意味し、現在のCD(Compact Disc)中心の音楽流通を大きく変えるものになる可能性を持っている。

15

ところで、音楽を鑑賞するスタイルという点に注目すると、自宅で鑑賞する以外にも、携帯型の再生装置を用いて、通勤、通学途中に鑑賞する、あるいは車の中で鑑賞するというスタイルもかなりの割合を占める。この場合には、音楽データをMD(Mini Disc)等の可搬型の媒体に記録する必要がある。

20

また、電子音楽配信においては、各社それぞれ独自の暗号方式を採用し、著作権保護を図っている。すなわち、製作会社、流通経路、利用形態等に応じて、それぞれ異なる暗号方式を採用している。このため、電子音楽配信によって音楽デ

25

ータをMD等に記録する場合、流通段階での音楽データをそのまま記録したとき、MD等を再生する再生装置は、各暗号方式に対応して復号化できる装置が求められる。この結果、装置規模が大きくなり、価格の上昇を招き、ユーザにとっては不利益となる。

- 5 一方、ユーザの利益だけを考えるなら、電子音楽配信された音楽データの暗号を復号化してMD等に記録するようにすれば、再生装置は、暗号解読を必要としないので安価なものを提供できることになる。

しかしながら、この場合には、不正なコピーを助長して著作権保護を図ることができない。

10

発明の開示

本発明は、上記課題に鑑みなされたものであり、著作権保護を図り、かつ記録媒体に記録された音楽データを安価なデジタルデータ再生装置で再生することができるデジタルデータ記録装置及びその方法並びにコンピュータ読み取り可能な記録媒体を提供することを目的とする。

15

上記目的は、デジタルデータを記録媒体に記録するデジタルデータ記録装置において、暗号化されたデジタルデータをデジタルネットワークを介して受信する通信手段と、前記通信手段により受信された暗号化デジタルデータを復号する復号化手段と、複数の暗号化部を有し、当該暗号化部はそれぞれ異なる

20 セキュリティレベルを有する暗号化方式の一つでデジタルデータを暗号化する暗号化手段と、前記暗号化手段により暗号化されたデジタルデータを前記記録媒体に記録する記録手段と、前記復号化手段と前記暗号化手段とを制御する制御手段とを備え、前記制御手段は、前記複数の暗号化部の一つで、前記復号化手段により復号化されたデジタルデータを再暗号化させることで達成できる。

25

このような構成によって、再生装置で容易に再生できる暗号化部で再暗号化されたデジタルデータを記録媒体に記録することができ、かつ暗号化されている

ので著作権の保護を図ることができる。

ここで、前記記録媒体に記録されたデジタルデータは、再生装置により再生され、前記暗号化手段は、前記記録媒体の識別情報を基に生成した暗号鍵によりデジタルデータを暗号化する第1暗号化部と、前記再生装置の識別情報を基に生成した暗号鍵によりデジタルデータを暗号化する第2暗号化部とを有し、前記制御手段は、前記記録媒体が再生装置から着脱可能か否かを判定し、着脱可能なときは、前記第1暗号化部によりデジタルデータの暗号化を行わせ、着脱不可能なときは、前記第2暗号化部によりデジタルデータの暗号化を行わせることができる。

- 10 このような構成によって、記録媒体がいずれかの再生装置で再生されるときには、その記録媒体の識別情報を基に生成される暗号鍵でデジタルデータを暗号化し、特定の一の再生装置で再生されるときには、その一の再生装置の識別情報を基に生成される暗号鍵でデジタルデータを暗号化することによって、記録媒体に記録されたデジタルデータを再生装置で再生することができる。

- 15 ここで、前記デジタルデータ記録装置は、更に、前記デジタルネットワークを介して課金処理を行う課金手段を備え、前記制御手段は、再暗号化を行う前記暗号化部の選択に基づいて課金値を決定し、決定した課金値に基づき課金処理を行うように前記課金手段を制御することができる。

- 20 このような構成によって、異なるセキュリティレベルを有する暗号化方式の暗号化部を選択することができ、かつ、暗号化部に応じた料金を支払うことができる。

ここで、前記制御手段は、前記暗号化手段が前記暗号鍵を生成できない場合は、受信された暗号化デジタルデータを、前記復号化手段により復号化することを禁止することができる。

- 25 このような構成によって、暗号化部で暗号鍵を生成できないときには、デジタルデータを復号する処理をなくすことができる。

ここで、前記暗号化手段の有する複数の暗号化部による暗号化されたデジタルデータは、前記通信手段により受信されたデジタルデータの暗号化に比べいずれもセキュリティレベルが低いとすることができる。

- このような構成によって、再生装置は、デジタルデータの再生が容易となり、
- 5 再生装置のコストダウンにつながる。

- ここで、前記通信手段により受信されるデジタルデータは異なるセキュリティレベルを有する暗号化方式の一つで暗号化されており、前記受信されるデジタルデータは当該デジタルデータの暗号化方式を示す属性情報を含み、前記復号化手段は、複数の復号化部を含み、当該復号化部は前記異なるセキュリティ
- 10 ベルを有する暗号化方式で暗号化されたデジタルデータをそれぞれ復号化し、前記制御手段は、前記通信手段により受信された暗号化デジタルデータの暗号化方式を前記属性情報に基づいて判定し、判定した暗号化方式に対応する前記復号化部により前記暗号化デジタルデータを復号化するように前記復号化手段を制御することができる。

- 15 このよな構成によって、受信されたデジタルデータごとに異なるセキュリティレベルを有する暗号化方式で暗号化されていても、暗号化方式に対応した復号化部を選んで、復号化することができる。

- ここで、前記デジタルデータ記録装置は、更に、前記デジタルネットワークを介して課金処理を行う課金手段を備え、前記制御手段は、受信した暗号化
- 20 デジタルデータに対し、復号化を行う前記復号化部の選択と再暗号化を行う前記暗号化部の選択とに基づいて課金値を決定し、決定した課金値に基づき課金処理を行うように前記課金手段を制御することができる。

このような構成によって、デジタルデータの復号化と再暗号化とに対応した利用料金が徴収され、著作権の保護を図ることができる。

- 25 また、上記目的は、デジタルデータを記録媒体に記録するデジタルデータ記録方法において、暗号化されたデジタルデータをデジタルネットワークを

介して受信する通信ステップと、前記通信ステップにより受信された暗号化デジタルデータを復号する復号化ステップと、複数の異なるセキュリティレベルを有する暗号化方式の一つで復号化されたデジタルデータを暗号化する暗号化ステップと、前記暗号化ステップにより暗号化されたデジタルデータを前記記録媒体に記録する記録ステップとを有することが達成できる。

このような構成によって、再生装置で容易に再生できる暗号化方式で暗号化されたデジタルデータを記録媒体に記録することができ、かつ、暗号化されているので著作権の保護を図ることができる。

ここで、前記通信ステップにより受信されるデジタルデータは異なるセキュリティレベルを有する暗号化方式の一つで暗号化されており、前記受信されるデジタルデータは当該デジタルデータの暗号化方式を示す属性情報を含み、複数の暗号化方式から一の暗号化方式を前記属性情報に基づいて判定する判定ステップを更に有し、前記復号化ステップは、前記判定ステップに従い暗号化されたデジタルデータを復号化することができる。

このような構成によって、通信手段で受信された暗号化されたデジタルデータが異なるセキュリティレベルを有する暗号化方式で暗号化されていても、復号化することができる。

また、上記目的は、デジタルデータを第1記録媒体に記録するデジタルデータ記録装置に適用されるコンピュータ読み取り可能な記録媒体において、暗号化されたデジタルデータをデジタルネットワークを介して受信する通信ステップと、前記通信ステップにより受信された暗号化デジタルデータを復号する復号化ステップと、複数の異なるセキュリティレベルを有する暗号化方式の一つで復号化されたデジタルデータを暗号化する暗号化ステップと、前記暗号化ステップにより暗号化されたデジタルデータを前記第1記録媒体に記録する記録ステップとの各ステップをコンピュータに実行させるプログラムを記録したコンピュータ読み取り可能な記録媒体で達成できる。

このような構成によって、容易に再生できる暗号化方式で暗号化されたデジタルデータを記録媒体に記録し、かつ、著作権の保護を図る機能のないデジタルデータ記録装置に適用して、このような機能を発揮させることができる。

- ここで、前記通信ステップにより受信されるデジタルデータは異なるセキュリティレベルを有する暗号化方式の一つで暗号化されており、前記受信されるデータは当該データの暗号化方式を示す属性情報を含み、複数の暗号化方式から一の暗号化方式を前記属性情報に基づいて判定する判定ステップを更に有し、前記復号化ステップは、前記判定ステップに従い暗号化されたデジタルデータを復号化することをコンピュータに実行させるプログラムを記録した請求の範囲第 11 項に記載のコンピュータ読み取り可能な記録媒体とすることができる。

このような構成によって、通信手段で受信された暗号化されたデジタルデータが異なるセキュリティレベルを有する暗号化方式で暗号化されていても復号化することができる。

15 図面の簡単な説明

図 1 は、本発明に係るデジタルデータ記録装置の実施の形態 1 の構成図である。

図 2 は、上記実施の形態のハード構成を示す外観図及び上記実施の形態で得られた記録媒体の再生装置の外観図である。

- 20 図 3 は、上記実施の形態の音楽データの購入のために開設されたホームページの表示画面の一例を示す図である。

図 4 は、上記実施の形態の一次記録媒体にダウンロードされた音楽データのデータ構造の一例を示す図である。

- 25 図 5 は、上記実施の形態の音楽データの購入のために開設されたホームページの表示画面の他の一例を示す図である。

図 6 は、上記実施の形態の動作を説明するフローチャートのその 1 である。

図 7 は、上記実施の形態の動作を説明するフローチャートのその 2 である。

図 8 は、本発明に係るデジタルデータ記録装置の実施の形態 2 の構成図である。

図 9 は、上記実施の形態の情報提供者が提供するデジタル信号を記録する際
5 の表示部に表示される情報を示す図である。

図 10 は、上記実施の形態の動作を示すフローチャートである。

図 11 は、本発明に係るデジタルデータ記録装置の実施の形態 3 の構成図である。

図 12 は、上記実施の形態の情報提供者が提供するデジタル信号の属性情報
10 のデータ構造を示す図である。

図 13 は、上記実施の形態の動作を示すフローチャートのその 1 である。

図 14 は、上記実施の形態の動作を示すフローチャートのその 2 である。

図 15 は、本発明に係るデジタルデータ記録装置の実施の形態 4 の構成図である。

15 図 16 は、本発明に係るデジタルデータ記録装置の実施の形態 6 の構成図である。

図 17 は、上記実施の形態のデジタルデータに付されて送信される属性情報のデータ構造の一例を示す図である。

図 18 は、上記実施の形態の記録媒体に記録される管理情報のデータ構造の一例を示す図である。
20

図 19 は、上記実施の形態の動作を説明するフローチャートである。

図 20 は、上記実施の形態で記録された記録媒体を再生するデジタルデータ再生装置の構成図である。

図 21 は、上記デジタルデータ再生装置の動作を説明するフローチャートである。
25

図 22 は、本発明に係るデジタルデータ記録装置の実施の形態 7 の構成図で

ある。

図 2 3 は、上記実施の形態のデジタルデータに付されて送信される属性情報のデータ構造の一例を示す図である。

図 2 4 は、上記実施の形態の動作を説明するフローチャートである。

- 5 図 2 5 は、上記実施の形態 7 の変形例のデジタルデータに付されて送信される属性情報のデータ構造の一例を示す図である。

発明を実施するための最良の形態

- 10 以下、本発明に係るデジタルデータ記録装置の実施の形態について図面を用いて説明する。

(実施の形態 1)

- 図 1 は、本発明に係るデジタルデータ記録装置の実施の形態 1 の構成図である。このデジタルデータ記録装置は、データ送受信部 1 0 0 と、受付部 1 0 1 と、一次記録媒体 1 0 2 と、データ取出部 1 0 3 と、判定部 1 0 4 と、復号化部群 1
15 0 5 と、暗号方式指示部 1 0 9 と、暗号化部群 1 1 0 と、二次記録媒体 1 1 4 と、記録部 1 1 5 と、固有情報取得部 1 1 6 と、指示受付部 1 1 7 と、課金部 1 1 8 とを備えている。

- なお、このデジタルデータ記録装置の二次記録媒体 1 1 4 と記録部 1 1 5 以外は、一般には図 2 に示すように P C (パーソナルコンピュータ) 2 0 1 で実現
20 され、記録部 1 1 5 は、例えば D V D (Digital Versatile Disc)-RAM ドライブ 2 0 2 で、二次記録媒体 1 1 4 は、D V D -RAM ディスク 2 0 3 でそれぞれ実現される。

- このデジタルデータ記録装置は、インターネットを介して配信される暗号化されたデジタルデータである音楽データを受信し、一次記録媒体 1 0 2 にダウンロードした後、復号化部群 1 0 5 でデジタルデータを復号化し、暗号化部群
25 1 1 0 で再度暗号化したデジタルデータとして、記録部 1 1 5 で二次記録媒体

1 1 4 に記録する。

なお、本実施の形態では、電子音楽配信について説明するけれども、デジタルデータの種類は、音楽データに限るものではなく、映像データ、文字データあるいはこれらの組み合わせでもよい。

- 5 データ送受信部 1 0 0 は、モデムと制御ソフトで実現される通信部であり、電話回線を通じて情報提供者のホストコンピュータ（図示せず）に接続される。受付部 1 0 1 で受け付けられた希望する曲の購入要求をデータ取出部 1 0 3 を介して通知されると、ホストコンピュータに送信する。インターネットを介して、ホストコンピュータから購入要求に従い配信される音楽データをダウンロードし、
- 10 一次記録媒体 1 0 2 に記録する。また、曲を購入したときに生じる課金情報をホストコンピュータに送信する。

ここで、情報提供者が提供する情報について説明する。情報提供者は、曲販売のサイト、すなわち自社のホームページを開設しており、曲名、価格などユーザの購入時に必要な情報、あるいは購買意欲をかきたてる情報を提供している。ユーザは、これらの情報提供者が提供する情報に基づいて、好みの曲を購入する。

- 15 図 3 は、情報提供者が提供する情報、すなわち曲販売用のホームページの一例を示すものである。表示される情報としては、曲名 3 0 1、歌手名 3 0 2、収録時間 3 0 3、価格 3 0 4 などの内容からなる。ここで、曲名 3 0 1、歌手名 3 0 2 は、それぞれ、個々の音楽データの曲名、歌手名を表す情報である。収録時間
- 20 3 0 3 は、個々の曲の収録時間（再生時間）を示し、価格 3 0 4 は、個々の曲の販売価格を示している。これらの情報をもとに、ユーザは受付部 1 0 1 を通じて好みの曲を選択し、購入要求を通知することができる。もちろん、情報提供者が提供する情報は、図 3 に示すように、文字情報に限られるものではなく、ジャケットピクチャのような画像や、試聴用の音楽データであってもよいことは言うま
- 25 でもない。

受付部 1 0 1 は、キーボードやマウス等からなり、P C の表示画面に表示され

た図 3 に示した情報を見たユーザから音楽データの購入要求を受け付ける。受け付けた曲の購入要求は、データ取出部 103 を介して、データ送受信部 100 に通知される。

5 一次記録媒体 102 は、一般には PC のハードディスク等で実現され、データ送受信部 100 で受信された暗号化されたデジタルデータである音楽データを記憶している。また、一次記録媒体のセキュアな領域には、課金部 118 によって、ダウンロードされた音楽データを二次記録媒体 114 に記録したとき、例えば暗号化した課金データが記録される。

10 図 4 は、一次記録媒体 102 に記憶されているダウンロードした音楽データ、すなわち情報提供者が提供する音楽データのデータ構造の一例を示すものである。情報提供者が提供する音楽データは、大きく音楽データの曲名や歌手名、価格などの情報である属性情報 401 と、音楽データそのものである曲データ部 402 とから構成される。

15 属性情報 401 は、ISRC 情報 403、曲名 404、歌手名 405、価格 406、情報提供者名 407、暗号形式 408 から構成される。以下、これらの属性情報について説明する。

ISRC(International Standard Recording Code)情報 403 は、音楽データごとに割り当てられる固有の情報であって、国コード (2 つの ASCII 文字)、オーナーコード (3 つの ASCII 文字)、記録年 (数字 2 桁)、シリアル番号 (数字 5 20 桁) で構成される。曲名 404、歌手名 405 は、それぞれ音楽データの曲名、歌手名を表す文字情報である。価格 406 は、音楽データの価格を表す情報である。なお、本実施の形態では、ダウンロードした音楽データをデジタルデータ記録装置を用いて、二次記録媒体に記録したときに請求される金額を示している。

25 情報提供者名 407 は、音楽データの提供者名、あるいは著作権者名を示す情報である。つまり、ユーザが本デジタルデータ記録装置を用いて音楽データを記録したときに課金し、その金額をどの業者に振り分ければよいのかを示す情報

である。

- 暗号形式 408 は、ダウンロードした音楽データがどの暗号形式で暗号化されているかを示す情報である。すなわち音楽データは、情報提供者ごとに異なる暗号方式で暗号化されている。例えば、情報提供者 A、情報提供者 B、情報提供者 C が音楽データを提供する場合、情報提供者 A の提供する音楽データは A 方式で暗号化されており、情報提供者 B の提供する音楽データは B 方式で暗号化されており、情報提供者 C の提供する音楽データは C 方式で暗号化されている。なお、本実施の形態では、情報提供者の提供する情報が、さまざまな形式で暗号化されている場合に、それを記録した二次記録媒体 114 を再生装置で著作権の保護を図りつつ、容易に解読できる暗号形式に変換することが発明の主たる目的であり、暗号化のアルゴリズムの詳細な説明については省略する。

また、属性情報 401 においては、価格 406、情報提供者名 407 は改竄されると情報提供者が不利益を被るおそれがあるため、必要に応じて暗号化されている。

- データ取出部 103 は、暗号方式指示部 109 からデジタルデータの取り出し指示を受けると、一次記録媒体 102 から、まず属性情報 401 を取り出し、属性情報 401 を課金部 118 に通知する。また、属性情報 401 中の暗号形式 408 の情報は、判定部 104 に通知する。なお、属性情報 401 中、価格 406 等が暗号化されているときは、復号化部群 105 によって、復号化してから課金部 118 に通知する。さらに一次記録媒体 102 から曲データ部 402 を取り出し、判定部 104 に出力する。データ取出部 103 で取り出されたデータは、すでに述べたように、情報提供者ごとに異なる暗号方式で暗号化されている。

- 判定部 104 は、データ取出部 103 から通知された暗号形式 408 の情報に基づいて、復号化部群 105 のいずれの復号化部に音楽データを出力するか判定する。

復号化部群 105 は、 n 個の復号化部よりなり、第 1 復号化部 106 は A 方

式で暗号化されたデジタルデータを復号し、第2復号化部107はB方式で暗号化されたデジタルデータを復号し、第n復号化部108はN方式で暗号化されたデジタルデータを復号する。各復号化部106～108は、情報提供者ごとの復号モジュールからなっている。

- 5 例えば、判定部104に通知された暗号形式408の情報がB方式であれば、判定部104は、音楽データの曲データ部402のデジタルデータを第2復号化部107に出力し、復号する。第2復号化部107は、入力されたデジタルデータを復号して、暗号方式指示部109に出力する。

- 10 第1から第n復号化部106～108のいずれかにより暗号化されたデータを復号する際、復号鍵が必要であればデータ送受信部100でデータの暗号方式に応じた復号鍵を入手し、データを復号化する。このようにして情報提供者ごとに異なる暗号方式で暗号化されているデータに対し、いったん各方式で暗号化されているデータを復号化する。

- 15 暗号方式指示部109は、指示受付部117から暗号方式の種類の指示を受け有的时候は、その指示に従った固有情報の取得を固有情報取得部116に指示する。固有情報取得部116から指示した固有情報の通知を受けたときは、データ取出部103に音楽データの取り出しを指示する。固有情報取得部116から指示に従った固有情報を取得できない旨の通知を受けたときには、表示部（図示せず）に指示された暗号方式の種類では暗号化できない旨を表示させる。また、
- 20 指示受付部117から暗号方式の種類の指示を受けていないときには、固有情報取得部116に二次記録媒体114の属性に従った固有情報の取得を指示する。固有情報取得部116から固有情報又は固有情報を取得できない旨を通知されると、データ取出部103に音楽データの取り出しを指示する。固有情報を取得できない旨の通知を受けたときには、乱数を発生する。

- 25 暗号方式指示部109は、指示受付部117から暗号方式の指示を受け付けているときは、その指示に応じた一の暗号化部を選び、復号化部群105のいずれ

かの復号化部 106、107、…、108 から復号されたデジタルデータの入力を受けると、固有情報取得部 116 から通知された固有情報とともに、復号されたデジタルデータを通知する。

- また、暗号方式指示部 109 は、指示受付部 117 から指示を受け付けていないときは、固有情報取得部 116 から通知された固有情報の種類に従い、一の暗号化部を選び、復号化部群 105 のいずれかの復号化部 106～108 から復号されたデジタルデータの入力を受けると、固有情報とともにデジタルデータを通知する。固有情報取得部 116 から固有情報を取得できない旨の通知を受けているとき、発生させた乱数とともに、一の暗号化部にデジタルデータを通知する。

- 暗号化部群 110 は、 n 個の暗号化部 111、112、…、113 からなる。各暗号化部 111、112、…、113 は、異なる種類の暗号鍵によって、通知されたデジタルデータを暗号化する。例えば、第 1 暗号化部 111 は、二次記録媒体 114 の固有の識別情報を基に作成される暗号鍵で暗号化する。第 2 暗号化部 112 は、二次記録媒体 114 を再生する再生装置（図示せず）の固有の識別情報を基に作成される暗号鍵で暗号化する。第 n 暗号化部 113 は、乱数を基に作成される暗号鍵で暗号化する。暗号化部 111～113 で用いられる各暗号鍵のデータサイズは、一次記録媒体 102 に記憶されている暗号化されたデジタルデータの暗号鍵のデータサイズよりも小さく設定される。

- 二次記録媒体 114 に記録される暗号化されたデジタルデータの暗号鍵のデータサイズが小さいことは、このデジタルデータを解読する際の困難性が低いことを意味する。したがって、二次記録媒体 114 を再生する再生装置でのデジタルデータの復号化に要する構成が簡単化されることになり、再生装置のコスト減につながる。

- 例えば、指示受付部 117 からの指示がないときに、暗号方式指示部 109 が固有情報取得部 116 から二次記録媒体の識別情報の通知を受けているときには、

第1暗号化部111に二次記録媒体の識別情報を通知する。第1暗号化部111は、その識別情報を基に暗号鍵を作成し、暗号方式指示部109から通知された音楽データの属性情報401の暗号形式408を書き換えるとともに、曲データ部402を、生成した暗号鍵で暗号化する。暗号化したデジタルデータを記録部115に通知する。

また、暗号方式指示部109は、指示受付部117から二次記録媒体114を再生する再生装置（図示せず）の固有情報による暗号化の指示を受けると、固有情報取得部116に再生装置の固有の識別情報を取得するよう指示する。固有情報取得部116から再生装置の固有の識別情報を通知されると、その識別情報と復号化部群105から通知された復号されたデジタルデータとを第2暗号化部112に通知する。

第2暗号化部112は、暗号方式指示部109から通知された識別情報を基に暗号鍵を生成し、生成した暗号鍵でデジタルデータを暗号化して記録部115に通知する。この際、音楽データの属性情報401の暗号形式408の内容を書き換えるのは、指示受付部117から指示を受け付けないときと同様である。

二次記録媒体114は、例えば図2に示したDVD-RAMディスク、MD、再生装置（図示せず）の機種により埋め込み型あるいは取り外し可能な型の小型の半導体メモリ等からなり、暗号化部群110で暗号化された音楽データが記録部115によって記録される。例えば、DVD-RAMディスク203にデジタルデータが記録されていれば、図2に示すように、DVD-Audioプレーヤ204にDVD-RAMディスク203を挿入して音楽を聴取することができる。

記録部115は、例えば、図2に示したDVD-RAMドライブ202で実現され、暗号化部群110から通知されたデジタルデータを二次記録媒体114に記録する。また、記録が終了すると、その旨、課金部118に通知する。

固有情報取得部116は、暗号方式指示部109から二次記録媒体114の固有の識別情報の取得を指示されたときには、例えば、DVD-RAMの場合は

BCA(Burst Cutting Area)に書かれている情報を読み出し、通知する。なお、この二次記録媒体 1 1 4 の固有の識別情報は、媒体ごとにユニークであり、通常ディスクの製造時に記録される情報であって、ユーザの通常の操作では読み出されたり、書き換えることができない。

- 5 したがって、この識別情報を基に暗号鍵を生成して、この暗号鍵で暗号化されたデジタルデータが DVD-RAM ディスクに記録されるので、万一悪意を持ったユーザがビットコピー可能なツールを用いて DVD-RAM ディスクの内容を複製し、再生しようとしても、復号鍵の基になる情報が異なるため、正常に復号化することができない。この結果、音楽データの著作権を確実に保護することができ
- 10 きる。

- また、暗号方式指示部 1 0 9 から二次記録媒体 1 1 4 が装着された再生装置（図示せず）の固有の識別情報の取得を指示されたときには、固有情報取得部 1 1 6 は、再生装置の識別情報を読み出し、暗号方式指示部 1 0 9 に通知する。この再生装置の固有の識別情報も再生装置の製造時に付される装置ごとのユニーク
- 15 な識別情報であるので、ユーザの通常の操作では読み出されたり、書き換えられたりすることはできない。したがって、この識別情報を基に暗号化された場合も、特定の再生装置でしか再生することができない。

- なお、固有情報取得部 1 1 6 は、暗号方式指示部 1 0 9 から指示された固有の識別情報を取得できないとき、即ち、二次記録媒体 1 1 4 又は再生装置に識別情報
- 20 が付されていない場合には、指示された種類の固有の識別情報を取得できない旨を暗号方式指示部 1 0 9 に通知する。

- 固有情報取得部 1 1 6 は、暗号方式指示部 1 0 9 から固有情報の種類の指示を受けずに、固有情報の取得の指示を受けると、二次記録媒体 1 1 4 が DVD-RAM ディスクなどの再生装置から取り外し可能なものであるか、それとも、小型の半導体メモリのような再生装置に埋め込まれた取り外し不可能ものであるか
- 25 を判断し、取り外し可能なものであれば、その二次記録媒体 1 1 4 の固有の識別

情報を読み出し、暗号方式指示部 109 に二次記録媒体 114 の識別情報を通知し、取り外し不可能なものであれば、再生装置の識別情報を読み出し、同様に再生装置の識別情報を通知する。識別情報を取得できないときは、その旨を暗号方式指示部 109 に通知する。

- 5 指示受付部 117 は、PC のキーボードやマウスで実現され、ユーザから暗号方式の種類を指示を受け付け、暗号方式指示部 109 に通知する。

先に述べた図 3 に示すホームページの情報では、販売価格は 1 通りしかなかったけれども、図 5 に示すようなホームページの内容であれば、価格 (1) 501、価格 (2) 502 の 2 通りの販売価格が示されている。

- 10 価格 (1) 501 は、二次記録媒体 114 の固有の識別情報を基にデジタルデータを暗号化して記録するときの価格を示しており、価格 (2) 502 は、二次記録媒体 114 を再生する再生装置の固有の識別情報を基にデジタルデータを暗号化して記録するときの価格を示している。なお、これらの 2 種類の価格は、情報提供者側でそれぞれ個別に自由に設定可能である。

- 15 ユーザは、指示受付部 117 から二次記録媒体 114 の利用形態に応じて、図 5 に示す曲情報あるいはその価格情報を参照して好みの暗号形態でデジタルデータを暗号化することを指示することができる。例えば、特定の再生装置でのみ再生するとき、即ち、他の再生装置で二次記録媒体 114 を再生しないときには、再生装置の固有の識別情報を基に暗号化することを指示する。図 5 に示すように
- 20 再生装置の識別情報を基に暗号化するほうが、価格 (2) 502 に示すように一般的に安価である。これは、他の再生装置で再生することができないので、二次記録媒体 114 の固有の識別情報を基に暗号化するよりも自由度が低いからである。ユーザは、自由に再生装置を選んで再生したいときには、二次記録媒体 114 の識別情報を基に暗号化するよう指示すればよい。

- 25 なお、指示受付部 117 と上述の受付部 101 とは、一体として構成されているけれども、説明上、2 つの構成要素として説明した。

課金部 118 は、データ取出部 103 から音楽データの属性情報 401 の通知を受け、記憶している。記録部 115 から暗号化されたデジタルデータを二次記録媒体 114 に記録した旨の通知を受けると、属性情報中の価格 406 を参照して課金額を決定し、一次記録媒体 102 のセキュアな領域に属性情報 401 とともに課金情報として書き込む。

なお、価格 406 が図 5 に示したように価格 (1) 501、価格 (2) 502 のように複数あるときは、暗号方式指示部 109 から通知された第 1 から第 n 暗号化部 111 ~ 113 のいずれが利用されたかに従い課金額を決定する。

次に、本実施の形態の動作を図 6、図 7 のフローチャートを用いて説明する。

10 先ず、受付部 101 はユーザからのホームページ表示の要求を受け、データ送受信部 100 が音楽データを提供する情報提供者が開設するホームページにアクセスし、データ取出部 103 によって表示部 (図性せず) にホームページ (図 3、図 5 参照) を表示させる (S602)。

15 次に、データ取出部 103 は、受付部 101 からユーザの希望する音楽データの購入指示を待ち、指定された音楽データの配信を受けるようデータ送受信部 100 に指示する (S604)。データ送受信部 100 は、音楽データを受信すると、一次記録媒体 102 にダウンロードする (S606)。

ユーザは、ホームページの表示をみて、暗号方式の種類を二次記録媒体 114 の利用形態に応じて、指示受付部 117 から入力する。

20 暗号方式指示部 109 は、指示受付部 117 から暗号方式の種類 of 指示を通知されたか否か判断し (S608)、通知されたときは、指示された暗号方式の種類に用いる固有情報の取得を固有情報取得部 116 に指示する (S610)。固有情報取得部 116 から指示された固有情報を取得できない旨の通知を受けたか否かを判断し (S612)、その旨の通知を受けたときは、指示された暗号方式
25 の種類では暗号化できない旨を表示部 (図示せず) に表示させ (S614)、処理を終了する。指示した種類の固有情報の通知を受けたときには、データ取出部

103にデジタルデータの取り出しを指示する。

データ取出部103は、一次記録媒体102に記録されている音楽データを取り出す(S616)。

5 S608において、暗号方式指示部109は、指示受付部117から指示を通知されないと判断したとき、固有情報取得部116に固有情報の種類を指定しないで、固有情報の取得を指示する(S618)。

固有情報取得部116は、二次記録媒体114の属性(再生装置(図示せず)に装着された二次記録媒体114が取り外し可能か不可能か)を判断し、取り外し可能な二次記録媒体114のときは二次記録媒体114の識別情報を取得し、
10 取り外し不可能な二次記録媒体114のときは再生装置の識別情報を取得する(S620)。

暗号方式指示部109は、固有情報取得部116から取得された固有(識別)情報又は、固有情報を取得できなかったときはその旨の通知を受けると(S622)、データ取出部103にデジタルデータの取り出しを指示し、S616に
15 移る。

次に、判定部104は、データ取出部103で取り出された音楽データの属性情報401中の暗号形式408を参照して、復号化部群105のいずれの復号化部106～108で復号するかを判定する(S702)。

判定部104で判定された一の復号化部は、判定部104を介して入力された
20 デジタルデータを復号化し、復号したデジタルデータを暗号方式指示部109に出力する(S704)。

暗号方式指示部109は、既に固有情報取得部116から通知されている固有情報(取得できない旨の情報も含む)に従い、暗号化部群110の一の暗号化部を選び、固有情報(取得できない旨の情報に対しては発生した乱数)と復号化さ
25 れたデジタルデータとを通知する(S706)。

暗号方式指示部109から通知を受けた一の暗号化部は、固有(識別)情報に

に基づいて暗号鍵を生成し（乱数の通知に対しては乱数に基づいて暗号鍵を生成し）、デジタルデータを暗号化する。この際、属性情報 401 のうち暗号形式 408 の内容も書き換えられる（S708）。

- 記録部 115 は、第 1 ～ 第 n 暗号化部 111 ～ 113 のいずれかから通知されたデジタルデータを二次記録媒体 114 に記録し（S710）、記録が終了すると課金部 118 に通知する。

課金部 118 は、記録部 115 から通知を受けると、データ取出部 103 から通知されている価格 406 等に従い課金額を決定し、課金情報を一次記録媒体 102 に記録して（S712）処理を終了する。

- 10 上記実施の形態では、復号化部群 105 は、情報提供者ごとの復号モジュール（復号化部）からなるものとしたけれども、復号化部群は、音楽データの品質、例えば 24 ビットの L P C M (Liner Pulse Code Modulation)、M P 3 (Moving Picture Experts Group 1 Audio Layer 3) 等のデジタルデータ、に応じて各復号化部を設けてもよい。高品質の 24 ビットの L P C M は、解読の困難性の高い
- 15 暗号化されたデジタルデータとし、通常品質の M P 3 は解読の困難性の低い暗号化されたデジタルデータとしておき、第 1 復号化部は 24 ビットの L P C M のデジタルデータを復号し、第 2 復号化部は M P 3 のデジタルデータを復号するようにしてもよい。

- 上記実施の形態では、暗号化部群 110 は、固有情報の種類で各暗号化部を設けたけれども、上述した品質に対応して、第 1 復号化部で復号化されたデジタルデータは第 1 暗号化部で暗号化し、第 2 復号化部で復号化されたデジタルデータは第 2 暗号化部で暗号化し、第 n 復号化部で復号化されたデジタルデータは第 n 暗号化部で暗号化するようにしてもよい。この場合、第 1 暗号化部で暗号化に用いる暗号鍵のデータサイズは、第 2 暗号化部のそれよりも大きく、第 2 暗号化部のそれは第 n 暗号化部のそれよりも大きく設定する。そして、課金部は、
- 25 デジタルデータの復号化がされた復号化部と復号化されたデジタルデータを

再暗号化部がされた暗号化部とによって課金額を決定する。このようにすることによって、高品質の音楽データの方がより著作権の保護を確実なものとする事ができる。また、この際、価格についても情報提供者は高品質の音楽データに高価格を設定することができる。

- 5 なお、上記実施の形態のデジタルデータ記録装置は、図 1 にその構成図を示したけれども、各構成要素の機能をコンピュータに発揮させるプログラムをコンピュータ読み取り可能なフロッピーディスク等の記録媒体に記録しておき、著作権の保護機能を有しないデジタルデータ記録装置に摘要して著作権の保護機能を有する装置とすることができる。
- 10 また、本実施の形態では、デジタルデータはユーザが購入希望を出したときにホストコンピュータからダウンロードするとして説明を行ったが、購入するしないにかかわらず音楽データ、あるいは、属性情報のみをいったんユーザの PC 内の一次記録媒体 102 に記録しておき、一次記録媒体 102 に記録されているデジタルデータに対して購入手続きを行う形態も考えられる。
- 15 また、本実施の形態では、属性情報 401 は曲データ 402 と別個に記述するとして説明を行ったが、いわゆる Water Mark（電子すかし）の形式で曲データ 402 のデジタルデータ中に埋め込むことも可能である。
- また、本実施の形態において、復号化部群 105 と暗号化部群 110 との間の暗号方式指示部 109 を介してのデータ入出力に関しては特に言及はしていない
- 20 が、セキュリティ上、認証を行ってデータを送信するか、あるいは復号化部群 105、暗号方式指示部 109 及び暗号化部群 110 を 1 つのチップで実現する、といった方法で復号化されたデータの漏洩を防ぐようにしてもよい。
- また、課金情報を記録するときには、一次記録媒体 102 中のセキュアな領域に記録ずるとして説明を行ったが、課金情報に関しては、一次記録媒体 102 と
- 25 は別の IC カードなどの記録媒体を設け、これに記録することが可能である。
- 本実施の形態では、課金のタイミングについては、説明を省略したが、例えば、

デジタルデータを二次記録媒体 1 1 4 に記録するときに必ずホストコンピュータと接続していなければいけないとするか、課金額が一定の金額に達するとホストコンピュータに自動的に接続するか、あるいは、課金情報記録後、一定の日時が経過すると自動的にホストコンピュータに接続する、としてもよい。

- 5 更に、本実施の形態では、情報提供者が提供する情報を音声情報として説明したが、これに限るものではなく、映像情報、音声情報、文字情報、あるいは、映像情報と音声情報と文字情報との組み合わせたものなどでもよいことはもちろんである。

(実施の形態 2)

- 10 図 8 は、本発明に係わるデジタルデータ記録装置の実施の形態 2 の構成図である。このデジタルデータ記録装置は、一般にはパーソナルコンピュータで実現され、データ送受信部 2 1 0 1、一次記録媒体 2 1 0 2、データ取出部 2 1 0 3、暗号方式判定部 2 1 0 4、第 1 の復号化部 2 1 0 5、第 2 の復号化部 2 1 0 6、第 3 の復号化部 2 1 0 7、暗号化部 2 1 0 8、記録部 2 1 0 9、二次記録媒
15 体 2 1 1 0、入力部 2 1 1 1、表示部 2 1 1 2、記録媒体固有情報取得部 2 1 1 3 を備える。また、復号化部群 2 1 1 5 は、第 1 の復号化部 2 1 0 5、第 2 の復号化部 2 1 0 6、第 3 の復号化部 2 1 0 7 から構成されるが、復号化部は 3 つに限るものではなく、ここでは、複数の復号化部から構成されることを示している。

- 20 なお、本実施の形態では、以後、記録対象となるデータを音楽データであるとし、音楽データはインターネットを通じて配信されるものとする。また、情報提供者ごとに異なる暗号方式でデータを暗号化しているものとする。

- 情報提供者は、曲名、価格、コピー制御情報など（以後、属性情報と称する）購入時に必要な情報、あるいは購買意欲をかきたてる情報を音楽データに重畳または音楽データから分離して提供するものとするが、本実施の形態では、属性
25 情報を音楽データから分離して提供する形態について説明する。

データ送受信部 2 1 0 1 は、モデムで実現される通信部であり、電話回線を通

じて提供者のホストコンピュータ（図示せず）に接続される。まず、ユーザは情報提供者が提供する属性情報を取得する。データ送受信部 2101 により取得した属性情報は、一次記録媒体 2102 に記録され、その一部または全部が表示部 2112 に表示される。図 9 は、表示部 2112 に表示される情報の一例を示すものである。表示される情報としては、曲名 2201、曲名コード 2202、歌手名 2203、データ入手先 2204 などの内容からなる。ここで、曲名 2201、歌手名 2203 は、それぞれ音楽データに対する曲名、歌手名を表す情報である。曲名コード 2202 は、音楽データを他の音楽データと識別するための識別子であり、例えば I S R C (International Standard Recording Code) 情報が付される。これらの情報をもとに、ユーザは入力部 2111 を通じて好みの曲を選択し、購入要求を通知することができる。データ入手先 2204 は、本実施の形態では該当する曲が記録されている URL (Uniform Resource Locator) 情報とする。もちろん、曲名コード 2202 に I S R C 情報が付されていれば、曲名コード 2202 からデータ入手先を特定することも可能である。

15 入力部 2111 は、マウス、キーボード等から実現され、ユーザからの曲の購入の指示、すなわち記録指示を受け付け、データ送受信部 2101 に通知する。ユーザは表示部 2112 に表示された情報を元に、マウスでその曲名等をクリックして音楽データの記録を指示する。

入力部 2111 から音楽データの記録指示があると、データ送受信部 2101 から電話回線を通じて提供者のホストコンピュータから記録要求のあった曲をダウンロードする。この際に、属性情報中の URL 情報をもとに曲データの位置を特定する。ダウンロードされたデータはいったん一次記録媒体 2102 に記録される。

一次記録媒体 2102 は、一般にはパソコンのハードディスクであって、ユーザが購入を希望した音楽データを暗号化されたまま記録する。したがって以後の動作に関しては、必ずしも常に提供者のホストコンピュータと接続している必要

はない。

データ取出部 2103 は、一次記録媒体 2102 から記録対象となる音楽データを
取り出す。このとき、ユーザは表示部 2112 に表示される図 9 に示した情報
と同程度の情報をもとに、二次記録媒体 2110 へ記録する音楽データを入力
5 部 2111 を通じて選択する。データ取出部 2103 で取り出されたデータは、
各情報提供者ごとの暗号方式で暗号化されている。このため、適当な復号方式で
復号することを暗号方式判定部 2104 により判定する。具体的には、デジタル
データのヘッダ部に暗号方式を識別できる情報を付加して送信する、属性情報
に暗号方式を記述しておく、などの方法が考えられ、これらの値に応じて暗号方
10 式を判定する。

第 1 の復号化部 2105、第 2 の復号化部 2106、第 3 の復号化部 2107
は、各情報提供者ごとの復号方式が存在していることを示すものであって、必ず
しも 3 つに限られるわけではない。暗号方式判定部 2104 により適当な復号化
部を選択し、復号化部により暗号化されたデータを復号する。このとき、例えば
15 暗号方式判定部 2104 で取得したデータの暗号方式に応じた復号鍵を入手また
は生成し、復号化部はこの復号鍵をもとにデータを復号化する。したがって、異
なる暗号方式で暗号化されているデータに対し、いったん各方式で暗号化されて
いるデータを復号化することになる。

次に、暗号化部 2108 にて復号化されたデータの暗号化を行うが、ここでは、
20 記録媒体固有の固有情報を暗号鍵情報として暗号化を行うこととする。なお、記
録媒体固有情報をもとに暗号化を行う一の方法については、特開平 5-2578
16 公報に開示されているので、ここでは詳しい説明は省略する。

記録媒体固有情報取得部 2113 は、暗号化部 2108 からの指示に従い、二次
記録媒体 2110 から固有情報を取り出し、暗号化部 2108 へ伝達する。

25 暗号化部 2108 は、記録媒体固有情報取得部 2113 で取得した固有情報を
暗号鍵として、暗号化する。

ここで、二次記録媒体 2 1 1 0 固有の情報について説明する。

二次記録媒体 2 1 1 0 は、媒体ごとの固有の識別情報を持っている。これは例えば DVD-RAM (Digital Versatile Disc Random Access Memory) の場合、BCA (Burst Cutting Area) に書かれた情報に相当する。この情報は、ディスクごとにユニークであり、しかも通常ディスク製作時に記録される情報であって、書き換えることができない。したがって、万一悪意を持ったユーザがビットコピー可能なツールを用いてディスクの内容を複製したとしても、復号鍵のもとになる情報が異なるために復号化することができず、データの著作権を確実に保護することが可能となる。

10 記録部 2 1 0 9 は、暗号化されたデータを二次記録媒体 2 1 1 0 に記録する。

以上のように構成されたデジタルデータ記録装置について、以後図 1 0 のフローチャートを用いてその動作を説明する。

まず、データ送受信部 2 1 0 1 は、属性情報をダウンロードし (S 2 3 0 1)、ユーザからのデジタルデータの記録指示を待ち (S 2 3 0 2)、指示されたデジタルデータをダウンロードし、一次記録媒体 2 1 0 2 に記録する (S 2 3 0 3)。次に、ダウンロードしたデータの暗号方式を判定し、適当な復号化部 2 1 0 5 ~ 2 1 0 7 へ復号化を指示する (S 2 3 0 4)。復号化部 2 1 0 5 ~ 2 1 0 7 により復号化する (S 2 3 0 5)。暗号化部 2 1 0 8 は、復号化されたデータが入力されると、記録媒体固有情報取得部 2 1 1 3 から二次記録媒体 2 1 1 0 の固有情報を取得する (S 2 3 0 6)。取得した固有情報を暗号鍵の一部として暗号鍵を作成し、暗号化部 2 1 0 8 はデータを暗号化する (S 2 3 0 7)。記録部 2 1 0 9 は、暗号化されたデータを二次記録媒体 2 1 1 0 に記録し (S 2 3 0 8)、処理を終了する。

25 以上で、本発明の実施の形態 2 のデジタルデータ記録装置に関する説明を終わる。

次に、本発明の実施の形態 3 のデジタルデータ記録装置に関する説明を行う。

(実施の形態 3)

図 1 1 は、本発明に係わるデジタルデータ記録装置の実施の形態 3 の構成図である。このデジタルデータ記録装置は、一般にはパーソナルコンピュータで実現され、データ送受信部 2 1 0 1、一次記録媒体 2 1 0 2、データ取出部 2 1

5 0 3、暗号方式判定部 2 1 0 4、復号化部群 2 1 1 5、属性情報取得部 2 4 0 1、コピー制御情報検出判定部 2 4 0 2、コピー制御情報変換部 2 4 0 3、課金情報算出部 2 4 0 4、暗号化部 2 1 0 8、記録部 2 1 0 9、二次記録媒体 2 1 1 0、入力部 2 1 1 1、表示部 2 1 1 2、記録媒体固有情報取得部 2 1 1 3 を備える。

10 なお、実施の形態 3 では、実施の形態 2 のデジタルデータ記録装置の各構成部分と同一の部分には同一の符号を付して、その説明を省略し、本実施の形態固有の部分について説明する。

まず、本実施の形態において、記録対象となるデータの属性情報が図 1 2 の通りであるとする。図 1 2 に示す属性情報は、図 9 に示す属性情報に加えて、コピー制御情報 2 5 0 1、課金情報 2 5 0 2 等の情報がある。ここで、コピー制御情報 2 5 0 1 は、コピーが許可されている世代数、あるいは回数の情報からなる。15 例えば世代数に関しては、「無制限にコピー可」、「1 世代だけコピー可（孫コピー禁止）」、「コピー禁止」等の値を取る。一方、回数に関しては、コピー許可されている回数のことで、0 以上の整数値を取りうる。例えば「孫コピー不可」は、二次記録媒体 2 1 1 0 にデジタルデータを記録後、二次記録媒体 2 1 1 0 中の20 データをもとにコピーすることを許可しないことを意味する。「無制限に許可」は、特に制限しないことを意味する。「2 回コピー可」など、コピーの回数の情報が含まれる場合は、二次記録媒体 2 1 1 0 に記録できる回数を意味する。

属性情報取得部 2 4 0 1 は、一次記録媒体 2 1 0 2 から、再生すべきデータに対応する属性情報を取得する。ここでは、コピー制御情報と課金情報を取り出す。25 なお、属性情報は著作権保護情報や課金情報を含むので、一次記録媒体 2 1 0 2 中のセキュアな領域に記録して、ユーザの通常の操作ではアクセスできないこと

が望ましい。

コピー制御情報検出判定部 2402 は、属性情報中のコピー制御情報を取り出し、以後のコピーが許可されているかどうか、許可されているとすればその世代数、あるいは回数の情報を取得する。

- 5 コピー制御情報検出判定部 2403 は、コピーが許可されている場合、コピー制御情報を必要に応じて書き換える。例えば、孫コピーが禁止されているときは、コピー制御情報の値を以後のコピーを禁止するように変更し、コピー許可回数が制限されているときは、許可回数から「1」減じた値に変更する。

- 10 ここで重要となるのは、コピー許可回数が設定されているとき、一般に、一次記録媒体 2102 に記録されたデータを何回二次記録媒体 2110 にコピーさせるかという数値であるため、コピー制御情報の書き換え対象となるのは、一次記録媒体 2102 中に記録されているデータである。したがって、一次記録媒体 2102 中に記録されている。コピー許可回数を「1」減じた値に変換し、二次記録媒体 2110 に記録すべきコピー許可回数は 0 として記録する。

- 15 課金情報算出部 2404 は、属性情報取得部 2401 で取得した属性情報から該当する曲の課金情報を取得し、これをもとに課金額を算出し、一次記録媒体 2102 中のセキュアな領域に記録する。

以上のように構成されたデジタルデータ記録装置について、以下、図 13 および図 14 のフローチャートを用いてその動作を説明する。

- 20 まず、データ送受信部 2101 は、属性情報をダウンロードし (S2601)、ユーザからのデジタルデータの記録指示を待ち (S2602)、指示されたデジタルデータをダウンロードし、一次記録媒体 2102 に記録する (S2603)。次に、記録対象となるデータの属性情報を属性情報取得部 2401 により取得する (S2604)。コピー制御情報判定部 2402 により属性情報中のコピー制御情報を判定し、コピーが許可されているかどうかを判定する (S2605)。コピーが許可されているときは、コピーが許可されている世代、回数の情

報を取得し、必要に応じてコピー制御情報変換部 2403 で書き換える (S2606)。コピーが許可されていない場合は、以後の処理を中断する (S2607)。次に暗号方式を判定し、復号化群 2115 中の適当な復号化部へ復号化を指示する (S2608)。復号化部 2105 ~ 2107 により復号化を行う (S2609)。復号化が終わると、属性情報取得部 2401 で取得した属性情報中の課金情報から適切な課金額を算出する (S2610)。

暗号化部 2108 は、復号化されたデータが入力されると、記録媒体固有情報取得部 2113 から二次記録媒体 2110 の固有情報を取得する (S2611)。取得した固有情報を暗号鍵の一部として暗号鍵を作成し、暗号化部 2108 はデータを暗号化する (S2612)。記録部 2109 は、暗号化されたデータを二次記録媒体 2110 に記録し (S2613)、処理を終了する。

以上で、本発明の実施の形態 3 に関する説明を終わる。

(実施の形態 4)

次に、本発明に係わるデジタルデータ記録装置の実施の形態 4 について説明する。このデジタルデータ記録装置は、実施の形態 2 とほぼ同一であるが、固有情報取得送出部 2803、記録部 2109、二次記録媒体 2110 が第 2 のデジタルデータ記録装置内にある点と、暗号鍵の情報のみが異なる。図 15 は、本発明に係わるデジタルデータ記録装置の実施の形態 4 の構成図である。このデジタルデータ記録装置は、第 1 のデジタルデータ記録装置 2800 と、第 2 のデジタルデータ記録装置 2801 とからなる。

第 1 のデジタルデータ記録装置 2800 は、データ送受信部 2101、一次記録媒体 2102、データ取出部 2103、暗号方式判定部 2104、復号化部群 2115、暗号化部 2108、入力部 2111、表示部 2112、固有情報取得部 2802 備える。

第 2 のデジタルデータ記録装置 2801 は、固有情報取得送出部 2803、記録部 2109、二次記録媒体 2110 を備える。

なお、実施の形態 4 では、実施の形態 2 のデジタルデータ記録装置の各構成部分と同一の部分には同一の符号を付して、その説明を省略し、本実施の形態固有の部分について説明する。

- 暗号化部 2 1 0 8 へ復号化部群 2 1 1 5 にて復号されたデータが入力されると、
- 5 記録媒体固有情報取得部 2 8 0 2 は、第 2 のデジタルデータ記録装置 2 8 0 1 中の固有情報取得送出部 2 8 0 3 へ固有情報の送出要求を出す。固有情報取得送出部 2 8 0 3 は、第 2 のデジタルデータ記録装置 2 8 0 1 に装着されている二次記録媒体 2 1 1 0 の固有識別情報、あるいは第 2 のデジタルデータ記録装置 2 8 0 1 固有の識別情報、あるいはその両方を取得し、固有情報取得部 8 0 2 へ
- 10 送出する。

- 暗号化部 2 1 0 8 では、第 2 のデジタルデータ記録装置 2 8 0 1 に装着されている二次記録媒体 1 1 0 の固有識別情報、あるいは第 2 のデジタルデータ記録装置 8 0 1 固有の識別情報、あるいは、二次記録媒体 2 1 1 0 の固有識別情報と第 2 のデジタルデータ記録装置 2 8 0 1 固有の識別情報の組み合わせの情報
- 15 を暗号鍵の一部としてデータを暗号化し、第 2 のデジタルデータ記録装置 2 8 0 1 へ出力する。第 2 のデジタルデータ記録装置 2 8 0 1 中の記録部 2 1 0 9 は暗号化されたデータを二次記録媒体 2 1 1 0 へ記録する。

- なお、固有情報取得送出部 2 8 0 3 で取得送出する固有情報であるが、二次記録媒体 2 1 1 0 が第 2 のデジタルデータ記録装置 2 8 0 1 に固定的に設けられているときは、装置固有の識別情報とし、二次記録媒体 2 1 1 0 が着脱自在に設けられているときは、二次記録媒体 2 1 1 0 固有の固有情報、あるいは二次記録媒体 2 1 1 0 の固有識別情報と第 2 のデジタルデータ記録装置 2 8 0 1 固有の識別情報の組み合わせの情報とすることにより、より柔軟な暗号方式を使用することが可能になる。

- 25 以上で、実施の形態 4 の説明を終わる。

(実施の形態 5)

次に、本発明に係わるデジタルデータ記録装置の実施の形態 5 について説明する。このデジタルデータ記録装置は、実施の形態 2、3 および 4 とほぼ同一である。ここでは、実施の形態 4 の説明に用いた構成図、図 15 を用いて説明する。相違点は、二次記録媒体 2110 に応じた暗号形式を採用し、記録すること
5 である。つまり、DVD-RAM と半導体メモリとでは取り扱うデータの最小単位、暗号化データを書きこむデータ量の単位の単位が異なるため、固有情報取得部 2802 は、固有情報取得送出部 2803 から、媒体の情報も取得して、最適なデータの単位で暗号化を行なうことになる。このため、暗号化部 2108 が複数存在し、適切な暗号化部へ固有情報ならびに媒体情報も伝達するものである。以上
10 より、DVD-RAM に限らず、半導体メモリ、IC カード、ハードディスク等を二次記録媒体 2110 として使用することが可能となる。

以上で、実施の形態 5 の説明を終わる。

なお、上記実施の形態 2～5 は現状において最善の効果が期待できるシステム例として説明したにすぎない。本発明は、その要旨を逸脱しない範囲で実施変更
15 することができる。具体的には以下に示すような変更実施が可能である。

また、実施の形態 2～5 では、デジタルデータはユーザが購入希望を出したときにホストコンピュータからダウンロードするとして説明を行ったが、購入するしないにかかわらずいったんユーザの PC 内の一次記録媒体 2102 に記録しておき、一次記録媒体 2102 に記録されているデジタルデータに対して購入
20 手続きを行う形態も考えられる。

また、実施の形態 2～5 では、コピー制御情報を属性情報に記述するとして説明を行なったが、いわゆる Water Mark (電子すかし) の形式でデジタルデータ中に埋め込むことも可能である。

また、課金情報を記録するときには、一次記録媒体 2102 中のセキュアな領域に記録するとして説明を行なったが、課金情報に関しては、一次記録媒体 21
25 02 とは別の IC カードなどの記録媒体を設け、これに記録することが可能であ

る。

また、実施の形態 2～5 では、情報提供者が提供する情報を音声情報として説明したが、これに限るものでなく、映像情報、音声情報、文字情報、あるいは、映像情報と音声情報と文字情報の組み合わせたものなどでもよいことはもちろん

5 である。

(実施の形態 6)

図 16 は、本発明に係るデジタルデータ記録装置の実施の形態 6 の構成図である。

このデジタルデータ記録装置は、通信部 3101 と、記録媒体 3102 と、
10 受信データ記録判定部 3103 と、表示部 3104 と、入力操作部 3105 と、
記録媒体固有情報取得部 3106 と、暗号化部 3107 と、記録部 3108 と、
課金情報記録部 3109 と、課金情報記録媒体 3110 と、課金部 3111 とを
備えており、PC で実現される。

通信部 3101 は、モデムで実現され、電話回線を介してデータ提供者のホス
15 トコンピュータ（図示せず）及び課金センタ（図示せず）に接続される。ホス
トコンピュータからデジタルデータとその属性情報とを受信すると、受信データ
記録判定部 3103 に通知する。

また、通信部 3101 は、課金センタから利用料の問い合わせがあると、その
旨課金部 3111 に通知し、課金部 3111 から課金情報の通知を受けると、電
20 話回線を介して、課金センタに課金情報を通知する。

本実施の形態では、データ提供者が提供するデジタルデータを音楽データ
あるとして説明する。データ提供者は、提供する音楽データを必要に応じて暗号
化したデジタルデータとし、デジタルデータには、情報識別子が付されてい
る。情報識別子は、曲名コードであり、他の音楽と識別するためのものである。

25 また、デジタルデータには、属性情報が付加されている。属性情報は、デ
ジタルデータの利用料金等を示すものであり、どの情報提供者から提供された情

報であるかを示す情報も含まれている。

図 17 は、属性情報の内容の一例を示す図である。属性情報 3201 には、デジタルデータの曲名 3202、演奏者（歌手）3203、曲名コード 3204、記録料金 3205、1 回あたりの再生料金 3206、再生可能回数 3207、暗号状態 3208、コピー許可 3209 等の項目の内容が含まれる。

ここで、曲名 3202、演奏者 3203 は、表示部 3104 に表示して、ユーザがコピー（複製）をするか否かを指示する判断資料となるものである。曲名コード 3204 は、音楽データを他の音楽データと識別するための識別子であり、曲ごとにユニークなものであり、例えば I S R C（International Standard Recording Code）が付される。なお、このコードは国コード（2 つの A S C I I 文字）、オーナーコード（3 つの A S C I I 文字）、記録年（数字 2 桁）、シリアル番号（数字 5 桁）で構成されている。

記録料金 3205、1 回あたり再生料金 3206、再生可能回数 3207 等は、課金基準データを構成し、いずれもその音楽データの利用料金を算定する為の情報である。

記録料金 3205 は、通信部 3101 で受信されたデジタルデータを記録媒体 3102 に記録する際の料金である。1 回あたりの再生料金 3206 は、記録媒体 3102 に記録されたデジタルデータの再生 1 回あたりの料金を示している。再生可能回数 3207 は、記録媒体 3102 に記録されたデジタルデータの再生が許容される回数を示している。「100 回」と記録されているときには、100 回に限り再生できることを示している。また、再生回数が一定回数以上になると、その後の料金が不要となる買い取り形式の設定も可能である。

暗号状態 3208 は、暗号有無フラグであり、通信部 3101 で受信されたデジタルデータが暗号化されているか否かを示すものである。

コピー許可 3209 は、記録許可フラグであり、ユーザ側で記録する、即ち、記録媒体 3102 に受信された音楽データを記録することを許可するか否かを示

す情報である。「1回のみ可」とは、1度だけ記録することが許可され、「許可」は、何度でも記録することが許可されていることを示している。

なお、本発明は、受信された音楽データを記録媒体3102に記録（複製）し、再生するときの音楽の著作権保護を図ることを主目的としたものであるので、この音楽データをリアルタイムに聴取するだけが許可されている場合についての説明は、簡単にする。この場合は、コピー許可3209は、「不可」とされている。このデジタルデータ記録装置には、復号化部と出力部とがその構成から省略されているけれども、通信部3101で受信されたデジタルデータは復号化部で復号され、出力部から音楽が出力される。この際、課金基準データには、聴取料金が含まれている。

記録媒体3102は、書き換え可能な記憶部材からなり、装置本体に着脱可能に取り付けられており、例えば、DVD-RAM等で構成される。

記録媒体3102の書き換え不能なセキュアな領域には、記録媒体3102の固有情報が予め記録されている。

また、記録媒体3102には、記録部3108によって、暗号化部3107で暗号化されたデジタルデータが記録される。

更に、記録媒体3102には、記録されたデジタルデータの管理情報と属性情報とが記録部3108によって記録されている。

受信データ記録判定部3103は、通信部3101からデジタルデータとその属性情報3201との通知を受けると、その属性情報3201を最初に通知されたとき記憶し、属性情報のうち、曲名3202、演奏者3203、記録料金3205、1回あたり再生料金3206等を表示部3104に表示させ、デジタルデータを暗号化部3107に通知する。

入力操作部3105からコピー（複製）指示を受けると、指示された音楽の曲名コード3204のデジタルデータのコピーが可能か否かを属性情報3201のコピー許可3209を見て判断する。コピーが許可であれば、記録媒体固有情

報取得部 3106 に記録媒体 3102 の固有情報を取得するよう指示する。また、暗号化部 3107 に曲名コード 3204 と暗号状態 3208 を通知する。

コピーが不可であれば、表示部 3104 にその旨を表示させる。

受信データ記録判定部 3103 は、記録部 3108 からコピー終了の通知を受けると、記憶している属性情報 3201 の項目、コピー許可 3209 を書き換える。即ち、コピー許可 3209 が「1 回のみ」とされているときには「コピー不可」に、「何回のみ可」と数字が記録されているときには「1」を減じた数字にそれぞれ書き換える。なお、この属性情報 3201 を記憶する記憶領域は、EEPROM 内に設けられており、このデジタルデータ記録装置の電源がオフされた場合でも記憶内容は消失されない。

例えば、暗号化部 3107 に曲名コード 3204 の「song01」を通知した後に、記録部 3108 からコピー終了の通知を受けると、「song01」に対応する項目、コピー許可 3209 を「1 回のみ可」から「コピー不可」に書き換える。このようにすることによってデータ提供者の有する権利が侵されることを防止できる。

表示部 3104 は、液晶ディスプレイや CRT 等からなり、受信データ記録判定部 3103 の制御により、デジタルデータである音楽データの曲名等の表示や、コピーができない旨の表示をする。

入力操作部 3105 は、マウス等からなり、ユーザのコピー指示を受け付け、受信データ記録判定部 3103 に通知する。ユーザは、表示部 3104 に表示された曲名や演奏者の表示を見て、記録媒体 3102 にその音楽をダウンロードしようとするとき、マウスでその曲名等をクリックして、その音楽のコピーを指示する。

記録媒体固有情報取得部 3106 は、受信データ記録判定部 3103 から固有情報の取得指示を受けると、記録媒体 3102 のセキュアな領域に記録されている固有情報を読み出し、暗号化部 3107 に通知する。

暗号化部 3107 は、記録媒体固有情報取得部 3106 から通知された固有情報を基に暗号鍵を作成する。受信データ記録判定部 3103 から通知されたデジタルデータを作成した暗号鍵を用いて暗号化したデジタルデータを作成し、記録部 3108 に通知する。

- 5 なお、受信データ記録判定部 3103 から通知されたデジタルデータが暗号化されている旨の通知を受けている場合には、そのデジタルデータを復号化し、おいてもよいし、そのままの状態でもよい。

- 10 例えば、記録媒体 3102 に記録すべきデジタルデータ *dataA* を受信データ記録判定部 3103 から通知された場合に、記録媒体 3102 の固有情報を基に暗号鍵 *KM* を作成すると、暗号化したデジタルデータ *E (KM,dataA)* を作成する。他の記録媒体にデジタルデータ *dataA* を記録する場合には、その他の記録媒体の固有情報を基に暗号鍵 *K'M* を作成したときは、暗号化したデジタルデータ *E* は、*E (K'M,dataA)* となる。

- 15 ここで、デジタルデータの暗号化の技術については、特開平 5-257816 号公報に記載されている。

記録部 3108 は、暗号化部 3107 から通知された暗号化されたデジタルデータを記録媒体 3102 に記録する。この際、記録媒体 3102 に記録したデジタルデータの管理情報を作成して、記録媒体 3102 に記録する。

- 20 図 18 は、管理情報の一例を示す図である。管理情報 3301 には、記録したデジタルデータの識別子である曲名コード 3204 と、記録媒体 3102 に記録されたデジタルデータの記録開始アドレス 3302、記録終了アドレス 3303 とが対応して記録される。

記録媒体 3102 に記録されたデジタルデータを再生する際、この管理情報 3301 が参照される。

- 25 また、記録部 3108 は、記録媒体 3102 に暗号化されたデジタルデータ及び管理情報の記録が終了すると、受信データ記録判定部 3103 に記憶されて

いる記録したデジタルデータに対応する属性情報 3 2 0 1 を読み出し、記録媒体 3 1 0 2 に書き込む。更に、受信データ記録判定部 3 1 0 3 にコピー終了の通知をする。また、課金情報記録部 3 1 0 9 に、記録したデジタルデータの曲名コードを通知する。

5 課金情報記録部 3 1 0 9 は、記録部 3 1 0 8 から曲名コード 3 2 0 4 の通知を受けると、受信データ記録判定部 3 1 0 3 に記憶されている曲名コード 3 2 0 4 に対応する属性情報 3 2 0 1 の記録料金 3 2 0 5 を読み出し、記録料金が有料のときは、課金情報記録媒体 3 1 1 0 にその曲名コードと記録料金と記録日時等を課金情報として記録する。

10 課金情報記録媒体 3 1 1 0 は、RAM カード等からなり、記録媒体 3 1 0 2 にダウンロードしたデジタルデータの課金情報が課金情報記録部 3 1 0 9 によって記録される。

課金部 3 1 1 1 は、通信部 3 1 0 1 を介して課金センタ（図示せず）からの利用料の問い合わせがあると、課金情報記録媒体 3 1 1 0 に記録されている未決済
15 の課金情報を読み出し、通信部 3 1 0 1 に通知する。通知が終了すると、課金センタに通知済（決済）のフラグを課金情報記録媒体 3 1 1 0 に記録する。

次に、本実施の形態の動作を図 1 9 のフローチャートを用いて説明する。

10 先ず、受信データ記録判定部 3 1 0 3 は、ユーザからデジタルデータの記録指示を待ち（S 3 4 0 2）、指示されたデジタルデータのコピーが許可されているか否かを属性情報 2 0 1 を見て判断する（S 3 4 0 4）。否のときは、コピーが許可されていない旨を表示部 3 1 0 4 に表示させ（S 3 4 0 6）、処理を終了する。

25 コピーが許可されているときは、記録媒体固有情報取得部 3 1 0 6 は、記録媒体 3 1 0 2 のセキュアな領域に記録されている記録媒体 3 1 0 2 の固有情報を取得し、暗号化部 3 1 0 7 に通知する（S 3 4 0 8）。

暗号化部 3 1 0 7 は、固有情報を基に暗号鍵を作成し、デジタルデータを暗

号化する（S 3 4 1 0）。

記録部 3 1 0 8 は、暗号化されたデジタルデータを記録媒体 3 1 0 2 に記録する（S 3 4 1 2）。

次に、課金情報記録部 3 1 0 9 は、記録されたデジタルデータの記録料金が
5 有料か否かを判断する（S 3 4 1 4）。無料であれば、処理を終了し、有料であれば、課金情報記録媒体 1 1 0 に課金情報を記録して（S 3 4 1 6）、処理を終了する。

図 2 0 は、上述のデジタルデータ記録装置で記録媒体 3 1 0 2 に記録されたデジタルデータの再生装置の構成図である。

10 このデジタルデータ再生装置は、記録媒体 3 1 0 2 と、入力操作部 3 5 0 1 と、再生情報読出部 3 5 0 2 と、表示部 3 5 0 3 と、記録媒体固有情報取得部 3 5 0 4 と、復号化部 3 5 0 5 と、再生部 3 5 0 6 と、課金情報記録部 3 5 0 7 と、課金情報記録媒体 3 5 0 8 とを備えている。

記録媒体 3 1 0 2 は、上記デジタルデータ記録装置で暗号化されたデジタルデータと管理情報 3 3 0 1 と属性情報 3 2 0 1 とが記録された DVD-RAM
15 を識別する識別子である固有情報が記録されている。

入力操作部 3 5 0 1 は、ユーザから再生開始の指示を受けると、再生情報読出部 3 5 0 2 に初期起動の指示を与える。ユーザから曲名の指示を受けると、その曲名を再生情報読出部 3 5 0 2 に通知する。なお、初期起動の指示の他に記録媒
20 体 3 1 0 2 がこのデジタルデータ再生装置に挿入されたときにも自動再生モードの指示が再生情報読出部 3 5 0 2 に与えられる。

再生情報読出部 3 5 0 2 は、入力操作部 3 5 0 1 から初期起動の指示を受けると、記録媒体 3 1 0 2 に記録されている属性情報 3 2 0 1 を読み出し、その項目である曲名 3 2 0 2 及び演奏者 3 2 0 3 の一覧を表示部 3 5 0 3 に表示させる。

25 また、入力操作部 3 5 0 1 から曲名の指示又は、自動再生モードの指示を受けると、属性情報 3 2 0 1 の対応する再生可能回数 3 2 0 7 が「1」以上であるか

- 否かを判断する。再生可能回数 3 2 0 7 が「1」以上であれば、その曲名コード 3 2 0 4 を読み出し、管理情報 3 3 0 1 の記録開始アドレスから記録終了アドレスまでに記録された暗号化されたデジタルデータを読み出し、復号化部 3 5 0 5 に通知する。この際、記録媒体固有情報取得部 3 5 0 4 に固有情報を取得する
- 5 よう指示するとともに、課金情報記録部 3 5 0 7 に、曲名コード 3 2 0 4 と 1 回あたりの再生料金 3 2 0 6 とを通知する。更にデジタルデータの読み出しが終了すると、属性情報 3 2 0 1 の項目である再生可能回数 3 2 0 7 の数を「1」減じた数に書き換える。なお、再生可能回数 3 2 0 7 が「無限」の場合には、そのままにする。
- 10 再生情報読出部 3 5 0 2 は、再生可能回数が「1」未満であると判断したとき、表示部 3 5 0 3 に再生可能回数が越えた旨を表示させる。
- 表示部 3 5 0 3 は、液晶ディスプレイ等からなり、再生情報読出部 3 5 0 2 で読み出された曲名等を一覧表示する。また、再生可能回数を超えてのユーザからの曲名指定に対して、再生可能回数が越えた旨を表示する。
- 15 記録媒体固有情報取得部 3 5 0 4 は、再生情報読出部 3 5 0 2 から固有情報の取得を指示されると、記録媒体 3 1 0 2 のセキュアな領域から記録媒体 3 1 0 2 の識別子である固有情報を取得し、復号化部 3 5 0 5 に通知する。
- 復号化部 3 5 0 5 は、記録媒体固有情報取得部 3 5 0 4 から固有情報の通知と、再生情報読出部 3 5 0 2 から暗号化されたデジタルデータの通知とを受けると、
- 20 固有情報を基に復号鍵を作成して、暗号化されたデジタルデータを復号し、復号化したデジタルデータを再生部 3 5 0 6 に通知する。
- 再生部 3 5 0 6 は、復号化部 3 5 0 5 からデジタルデータの通知を受けると、デコードして音楽を再生する。音楽の再生を終了すると課金情報記録部 3 5 0 7 に再生終了を通知する。
- 25 課金情報記録部 3 5 0 7 は、再生部 3 5 0 6 から再生終了の通知を受けると、再生情報読出部 3 5 0 2 から通知されている曲名コード 3 2 0 4 と 1 回あたりの

再生料金 3206 と再生日時とを課金情報として課金情報記録媒体 3508 に記録する。なお、1 回あたりの再生料金 3206 が有料でなければ、記録はしない。

課金情報記録媒体 3508 は、RAM カード等からなり、課金情報を課金情報記録部 3507 によって記録される。

- 5 次に、このデジタルデータ再生装置の動作を図 21 に示すフローチャートを用いて説明する。

先ず、ユーザは、再生開始を入力操作部 3501 のリモコン等を用いて指示し、表示部 3503 に表示された曲名を指定する。再生情報読出部 3502 は、音楽の再生要求であるとし (S3602)、指定された曲名の再生可能回数が「1」

- 10 以上であるか否かを属性情報 3201 をみて判断する (S3604)。再生可能回数が「1」未満であれば、表示部 3503 に再生可能回数を超えた旨を表示させ (S3606)、処理を終了する。

再生可能回数が「1」以上の場合には、再生情報読出部 3502 は、記録媒体 3102 から暗号化されたデジタルデータを読み出し、復号化部 3505 に通

- 15 知する (S3608)。

記録媒体固有情報取得部 3504 は、記録媒体 3102 から固有情報を取得して復号化部 3505 に通知する (S3610)。

復号化部 3505 は、固有情報を復号鍵として暗号化されたデジタルデータを復号化する (S3612)。

- 20 再生部 3506 は、デジタルデータをデコードして音楽を再生出力する (S3614)。

課金情報記録部 3507 は、再生料金が有料であるか否かを判断し (S3616)、無料のときは何もせずに、有料のときは、課金情報を課金情報記録媒体 3508 に記録して (S3618)、処理を終了する。

- 25 (実施の形態 7)

図 22 は、本発明に係るデジタルデータ記録装置の実施の形態 7 の構成図で

ある。このデジタルデータ記録装置は、第1デジタルデータ記録装置3700と第2デジタルデータ記録再生装置3710とからなる。

第1デジタルデータ記録装置3700は、第1記録媒体3701と、通信部3101と、受信データ1次記録判定部3702と、表示部3104と、入力操作部3105と、1次記録部3703と、受信データ読出判定部3704と、固有情報取得部3705と、暗号化部3706と、課金情報記録部3109と、課金情報記録媒体3110と、課金部3111とを備えており、PCで実現される。

第2デジタルデータ記録再生装置3710は、固有情報取得送出部3707と、2次記録部3708と、第2記録媒体3709と、入力操作部3501と、再生情報読出部3502と、表示部3503と、復号化部3505と、再生部3506と、課金情報記録部3507と、課金情報記録媒体3508とを備えている。

なお、上記実施の形態6のデジタルデータ記録装置及びデジタルデータ再生装置の各構成部分と同一の部分には同一の符号を付して、その説明を省略し、
15 本実施の形態固有の部分についてのみ説明する。

まず、第1デジタルデータ記録装置3700について説明する。上記実施の形態6のデジタルデータ記録装置と異なるのは、第1記録媒体3701が本装置に固定的に設けられ、この第1記録媒体3701に記録されたデジタルデータが2次記録のために暗号化されて出力されることである。

20 第1記録媒体3701は、本装置3700内に固定的に設けられたハードディスク等の書き込み可能な記録部材からなる。第1記録媒体3701には、通信部3101で受信された音楽データであるデジタルデータとその管理情報とが1次記録部3703によって書き込まれる。

受信データ1次記録判定部3702は、通信部3101で受信されたデジタルデータに付された属性データをEEPROM内に設けられた記憶領域に書き込む。本実施の形態で受信される属性情報の一例を図23に示す。属性情報380

1 は、上記実施の形態 6 の属性情報 3 2 0 1 と 2 次記録料金 3 8 0 2 が記録されていることと、コピー許可（1 次） 3 8 0 3 と（2 次） 3 8 0 4 との記録の許可回数が示されていることとが異なる。

また、曲名コード「song05」の「曲 E」では、コピーが 1 次、2 次ともに不許可であり、リアルタイムの聴取のみが許可された音楽であることを示している。

受信データ 1 次記録判定部 3 7 0 2 は、ユーザからある音楽の 2 次記録の指示を受けると、まず 1 次記録が許可されているか否かを属性情報 3 8 0 1 の項目コピー許可（1 次） 3 8 0 3 を見て判断する。許可されていないときは、表示部 3 1 0 4 に不許可である旨を表示させる。許可されているときは、指示された音楽のデジタルデータを 1 次記録部 3 7 0 3 に通知する。他の機能は、上記実施の形態 6 の受信データ記録判定部 3 1 0 3 と同様である。

1 次記録部 3 7 0 3 は、通知されたデジタルデータを第 1 記録媒体 3 7 0 1 に記録する。この際、管理情報を書き込むのは、上記実施の形態 6 の記録部 3 1 0 8 と同様である。なお、上記実施の形態 6 では、記録媒体 3 1 0 2 の固有情報を基に暗号鍵が作成され、デジタルデータが暗号化されていたけれども、本実施の形態では、第 1 記録媒体 3 7 0 1 が取外され、他の装置で利用されることがないので暗号化されない。

また、1 次記録部 3 7 0 3 は、第 1 記録媒体 3 7 0 1 へのデジタルデータの記録が終了すると、受信データ読出判定部 3 7 0 4 に記録した曲名コード 3 8 0 5 を通知する。

受信データ読出判定部 3 7 0 4 は、1 次記録部 3 7 0 3 から曲名コード 3 8 0 5 の通知を受けると、その音楽の 2 次記録が許可されているか否かを、受信データ 1 次記録判定部 3 7 0 2 の属性情報 3 8 0 1 中のコピー許可（2 次） 3 8 0 4 を見て判断する。許可されていないとき、又は、許可回数が「1」以上でないときには、表示部 3 1 0 4 に 2 次記録が許可されていない旨を表示させる。

受信データ読出判定部 3 7 0 4 は、2 次記録が許可されているときには、管理

情報（図 18 参照）を見て、第 1 記録媒体 3701 に記録されている通知された曲名コードのデジタルデータを読み出して暗号化部 3706 に通知するとともに、固有情報取得部 3705 に固有情報を取得するよう指示する。

5 また、受信データ読出判定部 3704 は、デジタルデータの読み出しが完了すると、受信データ 1 次記録判定部 3702 に記憶されている属性情報 3801 のコピー許可（2 次）3804 の回数から「1」減じた数に書き換える。例えば「1 回のみ可」であれば「不許可」に書き換え、「許可」だけであれば、回数に制限がないので、そのまま書き換えは行わない。

10 なお、受信データ読出判定部 3704 は、暗号化部 3706 にデジタルデータの通知の後に、受信データ 1 次記録判定部 3702 に記憶されている属性情報を読み出して通知する。

固有情報取得部 3705 は、受信データ読出判定部 3704 から固有情報を取得するよう指示されると、第 1 デジタルデータ記録装置 3700 に接続されている第 2 デジタルデータ記録再生装置 3710 の固有情報取得送出部 3707
15 に、固有情報の送出を要求する。固有情報取得送出部 3707 から固有情報の通知を受けると、暗号化部 3706 に固有情報を通知する。

暗号化部 3706 は、固有情報取得部 3705 から通知された固有情報を基に暗号鍵を作成し、受信データ読出判定部 3704 から通知されたデジタルデータを暗号化して第 2 デジタルデータ記録再生装置 3710 の 2 次記録部 370
20 8 に送出する。この暗号化されたデジタルデータの送出の後に、通知された属性情報も送出する。

次に、第 2 デジタルデータ記録再生装置 3710 について説明する。この第 2 デジタルデータ記録再生装置 3710 は、携帯型の例えばヘッドホンステレオタイプの装置で実現される。また、第 2 記録媒体 3709 がこの装置 371
25 0 から着脱自在の半導体メモリの IC カード等から構成されている。

固有情報取得送出部 3707 は、第 1 デジタルデータ記録装置 3700 の固

有情報取得部 3705 から固有情報の送出要求を受けると、第 2 記録媒体 3709 に予め記録されている第 2 記録媒体固有の媒体識別情報と、この装置 3710 固有の機器識別情報とを取得して、固有情報取得部 3705 に通知する。また、再生情報読出部 3502 から固有情報の通知指示を受けると、復号化部 3505
5 に媒体識別情報と機器識別情報とを通知する。

2 次記録部 3708 は、第 1 デジタルデータ記録装置 3700 の暗号化部 3706 から暗号化されたデジタルデータと、属性情報との出力を受けると、第 2 記録媒体 3709 に記録する。併せて、図 18 に示したような管理情報 3301 を記録する。復号化部 3505 は、固有情報取得送出部 3707 から通知され
10 た媒体識別情報と機器識別情報との 2 つの情報を基に復号鍵を作成して、再生情報読出部 3502 から通知された暗号化されたデジタルデータを復号する。なお、その他の構成は、上記実施の形態 6 のデジタルデータ再生装置の構成とほぼ同様である。

次に、第 2 記録媒体 3709 がこの装置 3710 に固定的に設けられた IC カード等から構成される場合について述べる。この場合には、第 2 記録媒体 3709 がこの装置 3710 以外で再生されることがないことから固有情報取得送出部
15 3707 は、媒体識別情報を取得することなく、自ら記憶している機器識別情報を固有情報取得部 3705 に通知する。また、復号化部 3505 にも、機器識別情報を通知する。

20 このように、第 2 デジタルデータ記録再生装置 3710 に設けられた第 2 記録媒体 3709 が着脱自在であるか否かによって、デジタルデータの暗号化の暗号鍵の作成を媒体識別情報と機器識別情報との組合せによるか、機器識別情報だけで行うかを使い分けることができる。このように使い分けることによって、デジタルデータの不正な複製や不正な再生利用を防止することができる。

25 次に、本実施の形態の動作を図 24 に示すフローチャートを用いて説明する。まず、受信データ 1 次記録判定部 3702 は、入力操作部 3105 からディジタ

ルデータの2次記録の指示が有るのを待ち（S 3 9 0 2）、デジタルデータの1次記録が許可されているか否かを属性情報3 8 0 1を見て判断する（S 3 9 0 4）。許可されていないときは、その旨を表示部3 1 0 4に表示させて（S 3 9 0 6）、処理を終了する。

- 5 許可されているときは、受信データ1次記録判定部3 7 0 2は、デジタルデータを1次記録部3 7 0 3に通知する。1次記録部3 7 0 3は、第1記録媒体3 7 0 1にデジタルデータと管理情報とを記録する（S 3 9 0 8）。

次に、課金情報記録部3 1 0 9は、1次記録に対して課金されているか否かを判断し（S 3 9 1 0）、1次コピーが有料の時は課金情報を課金情報記録媒体3 1 1 0に記録する（S 3 9 1 2）。

次に、受信データ読出判定部3 7 0 4は、第1記録媒体3 7 0 1に記録されたデジタルデータの2次記録が許可されているか否かを受信データ1次記録判定部3 7 0 2に記憶されている属性情報3 8 0 1を見て判断する（S 3 9 1 4）。許可されていないときは、2次記録が許可されていない旨を表示部3 1 0 4に表示させ（S 3 9 1 6）、処理を終了する。

許可されているときは、受信データ読出判定部3 7 0 4は、第1記録媒体3 7 0 1からデジタルデータを読み出し、暗号化部3 7 0 6に通知するとともに、固有情報取得部3 7 0 5に第2デジタルデータ記録再生装置3 7 1 0から固有情報を取得するよう指示する。固有情報取得部3 7 0 5は、固有情報を取得し、暗号化部3 7 0 6に通知する（S 3 9 1 8）。暗号化部3 7 0 6は、通知された固有情報を基に暗号鍵を作成し（S 3 9 2 0）、通知されているデジタルデータを暗号化して第2デジタルデータ記録再生装置3 7 1 0の2次記録部3 7 0 8に出力する。

2次記録部3 7 0 8は、通知された暗号化されたデジタルデータと属性情報と管理情報とを第2記録媒体3 7 0 9に記録する（S 3 9 2 2）。

また、課金情報記録部3 1 0 9は、2次記録に対して課金されているか否かを判

断し（S 3 9 2 4）、2次記録が有料のときは、課金情報を課金情報記録媒体 1 1 0 に記録し（S 3 9 2 6）、処理を終了する。

なお、第2デジタルデータ記録再生装置 3 7 1 0 でのデジタルデータの再生動作は、実施の形態 6 のデジタルデータ再生装置の動作とほぼ同様であるの
5 で説明を省略する。

（変形例）

上記実施の形態 7 では、第2記録媒体 3 7 0 9 が着脱自在であるときには、第2デジタル記録再生装置 3 7 1 0 の機器識別情報と、第2記録媒体 3 7 0 9 の媒体識別情報とを組合せた暗号鍵でデジタルデータが暗号化されたけれども、
10 本変形例では、暗号化の形態（媒体識別情報のみに基づいた暗号鍵とするのか媒体識別情報に機器識別情報を組合せた暗号鍵とするのか）をユーザに指定させ、ユーザの利用形態の自由度を拡大している。即ち、第2デジタルデータ記録再生装置 3 7 1 0 で第2記録媒体 3 7 0 9 に記録された音楽を再生しようとするときには、媒体識別情報及び機器識別情報でデジタルデータを暗号化して記録する
15 ようにし、他のデジタルデータ再生装置（媒体識別情報を復号鍵として暗号化されたデジタルデータを復号化できる装置）で第2記録媒体 3 7 0 9 に記録された音楽を再生しようとするときには、媒体識別情報でデジタルデータを暗号化して記録するようにする。ユーザの利用形態に応じて暗号化の形態を選択できるようにしている。

20 一方、このユーザの利用の自由度に応じて2次記録料金を設定して、著作権の保護を図っている。

以下、本変形例の具体的構成を説明する。なお、本変形例は、図 2 2 に示した第1デジタルデータ記録装置 3 7 0 0 の構成に若干の機能を追加するものである
25 のので、実施の形態 7 の構成図をそのまま利用して、本変形例固有の構成についての説明する。

図 2 5 は、受信データ 1 次記録判定部 3 7 0 2 に記憶されている属性情報 3 1

001の一部を示している。この属性情報31001では、図23に示した属性情報3801の2次記録料金3802と2次記録料金31002との内容が異なる。

2次記録料金31002は、暗号化の暗号鍵が媒体識別情報（媒体ID）31003、機器識別情報（機器ID）31004、媒体識別情報と機器識別情報との組み合わせ31005のいずれであるかによって異なっている。媒体識別情報31003を基に暗号鍵が作成されたものでは、他の装置に第2記録媒体3709を装着して音楽を再生でき、ユーザの自由度が増すことから2次記録料金（2次複製利用料金）が機器識別情報31004又は媒体識別情報と機器識別情報との組み合わせ31005を基に暗号鍵が作成されたものよりも高額に設定される。ユーザの利用形態の拡大に応じて複製利用料金を課金できるようにしたものである。

固有情報取得部3705は、固有情報取得送出部3707から機器識別情報と媒体識別情報との通知を受けると、表示部3104に第2記録媒体3709を他の装置で利用するか、第2デジタルデータ記録再生装置3710でのみ利用するかを表示させ、ユーザの選択を待つ。

ユーザは、入力操作部3105より、他の装置を用いるか、第2デジタルデータ記録再生装置3710のみを用いるかを指定する。即ち、暗号鍵を媒体識別情報だけで作成するか、媒体識別情報と機器識別情報との組み合わせで作成するかを指示する。

入力操作部3105は、この指定を固有情報取得部3705と受信データ1次記録判定部3702とに通知する。

受信データ1次記録判定部3702は、入力操作部3105から他の装置を用いるとの通知を受けると、課金情報記録部3109に媒体識別情報31003を暗号鍵とする2次記録料金である旨を、第2デジタルデータ記録再生装置のみを用いるとの通知を受けると、媒体識別情報と機器識別情報との組み合わせ31005を暗号鍵とする2次記録料金である旨を通知する。

固有情報取得部 3705 は、入力操作部 3105 から、他の装置を用いる旨の通知を受けると、暗号化部 3706 に媒体識別情報のみを通知する。また、第 2 デジタルデータ記録再生装置 3710 でのみ用いる旨の通知を受けると、同様に媒体識別情報と機器識別情報とを通知する。

- 5 課金情報記録部 3109 は、暗号化部 3706 から暗号化されたデジタルデータを 2 次記録部 3708 に送出した旨の通知を受けると、受信データ 1 次記録判定部 3702 から通知されている属性情報 31001 の 2 次記録料金 31002 を見て、課金情報記録媒体 3110 に課金情報を記録する。

- 10 なお、本変形例において、第 2 記録媒体が着脱自在の DVD-RAM であるときには、上記実施の形態 6 と同様、DVD-RAM 固有の識別情報のみを基に暗号鍵を作成し、デジタルデータを暗号化して記録するようにできるのは勿論である。

また、本変形例の動作は、上記実施の形態 7 の動作と基本的に異なるところがないのでその説明は省略する。

- 15 なお、上記実施の形態 6、7 及び変形例において、課金情報記録媒体 3110、3508 は例えば IC カードにより実現し、デジタルデータの記録や再生時に IC カードをセットしなければ動作しないとすることも可能である。

- 20 また、上記実施の形態 6、7 及び変形例では、通信部 3110 で受信されるデジタルデータが音楽データであるとして説明したけれども、これに限ることはなく、映像データ、音声データ、文字データやこれらの組合せであってもよいのは勿論である。

- 25 上記実施の形態 6 と実施の形態 7 と変形例のデジタルデータ記録装置及び再生装置並びにデジタルデータ記録再生装置は、図 16、図 20 及び図 22 にその構成図を示したけれども、各構成要素の機能を発揮するプログラムをコンピュータ読取可能なフロッピーディスク等の記録媒体に記録しておき、著作権の保護機能を有しないデジタルデータ記録再生装置に適用して著作権の保護機能を有する装置とすることができる。

産業上の利用可能性

- 以上のように、本発明に係るデジタルデータ記録装置は、著作権保護を図り、再生装置の低コスト化を実現でき、種々の方式で暗号化されて電子配信されるデジタルデータの記録装置として有用であり、特に電子音楽配信される音楽データの記録装置として最適である。
- 5

請 求 の 範 囲

1. デジタルデータを記録媒体に記録するデジタルデータ記録装置において、
暗号化されたデジタルデータをデジタルネットワークを介して受信する通

5 信手段と、

前記通信手段により受信された暗号化デジタルデータを復号する復号化手段
と、

複数の暗号化部を有し、当該暗号化部はそれぞれ異なるセキュリティレベルを
有する暗号化方式の一つでデジタルデータを暗号化する暗号化手段と、

10 前記暗号化手段により暗号化されたデジタルデータを前記記録媒体に記録す
る記録手段と、

前記復号化手段と前記暗号化手段とを制御する制御手段とを備え、

前記制御手段は、前記複数の暗号化部の一つで、前記復号化手段により復号化
されたデジタルデータを再暗号化させることを特徴とするデジタルデータ記

15 録装置。

2. 前記記録媒体に記録されたデジタルデータは、再生装置により再生され、
前記暗号化手段は、

前記記録媒体の識別情報を基に生成した暗号鍵によりデジタルデータを暗号
20 化する第1暗号化部と、

前記再生装置の識別情報を基に生成した暗号鍵によりデジタルデータを暗号
化する第2暗号化部とを有し、

前記制御手段は、

前記記録媒体が再生装置から着脱可能か否かを判定し、着脱可能なときは、前
25 記第1暗号化部によりデジタルデータの暗号化を行わせ、着脱不可能なときは、
前記第2暗号化部によりデジタルデータの暗号化を行わせることを特徴とする

請求の範囲第 1 項に記載のデジタルデータ記録装置。

3. 前記デジタルデータ記録装置は、更に、

前記デジタルネットワークを介して課金処理を行う課金手段を備え、

5 前記制御手段は、再暗号化を行う前記暗号化部の選択に基づいて課金値を決定し、決定した課金値に基づき課金処理を行うように前記課金手段を制御することを特徴とする請求の範囲第 1 項に記載のデジタルデータ記録装置。

4. 前記記録媒体に記録されたデジタルデータは、再生装置により再生され、

10 前記暗号化手段は、

前記記録媒体の識別情報を基に生成した暗号鍵によりデジタルデータを暗号化する第 1 暗号化部と、

前記再生装置の識別情報を基に生成した暗号鍵によりデジタルデータを暗号化する第 2 暗号化部とを有し、

15 前記制御手段は、

前記記録媒体が再生装置から着脱可能か否かを判定し、着脱可能なときは、前記第 1 暗号化部によりデジタルデータの暗号化を行わせ、着脱不可能なときは、前記第 2 暗号化部によりデジタルデータの暗号化を行わせることを特徴とする請求の範囲第 3 項に記載のデジタルデータ記録装置。

20

5. 前記制御手段は、

前記暗号化手段が前記暗号鍵を生成できない場合は、受信された暗号化デジタルデータを、前記復号化手段により復号化することを禁止することを特徴とする請求の範囲第 4 項に記載のデジタルデータ記録装置。

25

6. 前記暗号化手段の有する複数の暗号化部による暗号化されたデジタルデー

タは、前記通信手段により受信されたデジタルデータの暗号化に比べいずれもセキュリティレベルが低いことを特徴とする請求の範囲第 1 項記載のデジタルデータ記録装置。

- 5 7. 前記通信手段により受信されるデジタルデータは異なるセキュリティレベルを有する暗号化方式の一つで暗号化されており、前記受信されるデジタルデータは当該デジタルデータの暗号化方式を示す属性情報を含み、

前記復号化手段は、複数の復号化部を含み、当該復号化部は前記異なるセキュリティレベルを有する暗号化方式で暗号化されたデジタルデータをそれぞれ復
10 号化し、

前記制御手段は、前記通信手段により受信された暗号化デジタルデータの暗号化方式を前記属性情報に基づいて判定し、判定した暗号化方式に対応する前記復号化部により前記暗号化デジタルデータを復号化するように前記復号化手段を制御することを特徴とする請求の範囲第 1 項に記載のデジタルデータ記録装
15 置。

8. 前記デジタルデータ記録装置は、更に、

前記デジタルネットワークを介して課金処理を行う課金手段を備え、

- 20 前記制御手段は、受信した暗号化デジタルデータに対し、復号化を行う前記復号化部の選択と再暗号化を行う前記暗号化部の選択とに基づいて課金値を決定し、決定した課金値に基づき課金処理を行うように前記課金手段を制御することを特徴とする請求の範囲第 7 項に記載のデジタルデータ記録装置。

9. デジタルデータを記録媒体に記録するデジタルデータ記録方法において、
25 暗号化されたデジタルデータをデジタルネットワークを介して受信する通信ステップと、

前記通信ステップにより受信された暗号化デジタルデータを復号する復号化ステップと、

複数の異なるセキュリティレベルを有する暗号化方式の一つで復号化されたデジタルデータを暗号化する暗号化ステップと、

- 5 前記暗号化ステップにより暗号化されたデジタルデータを前記記録媒体に記録する記録ステップとを有することを特徴とするデジタルデータ記録方法。

10 前記通信ステップにより受信されるデジタルデータは異なるセキュリティレベルを有する暗号化方式の一つで暗号化されており、前記受信されるデジ

- 10 タルデータは当該デジタルデータの暗号化方式を示す属性情報を含み、

複数の暗号化方式から一の暗号化方式を前記属性情報に基づいて判定する判定ステップを更に有し、

前記復号化ステップは、前記判定ステップに従い暗号化されたデジタルデータを復号化することを特徴とする請求の範囲第9項に記載のデジタルデータ記

- 15 録方法。

11 デジタルデータを第1記録媒体に記録するデジタルデータ記録装置に適用されるコンピュータ読み取り可能な記録媒体において、

- 20 暗号化されたデジタルデータをデジタルネットワークを介して受信する通信ステップと、

前記通信ステップにより受信された暗号化デジタルデータを復号する復号化ステップと、

複数の異なるセキュリティレベルを有する暗号化方式の一つで復号化されたデジタルデータを暗号化する暗号化ステップと、

- 25 前記暗号化ステップにより暗号化されたデジタルデータを前記第1記録媒体に記録する記録ステップとの各ステップをコンピュータに実行させるプログラム

を記録したコンピュータ読み取り可能な記録媒体。

12. 前記通信ステップにより受信されるデジタルデータは異なるセキュリティレベルを有する暗号化方式の一つで暗号化されており、前記受信されるデータ

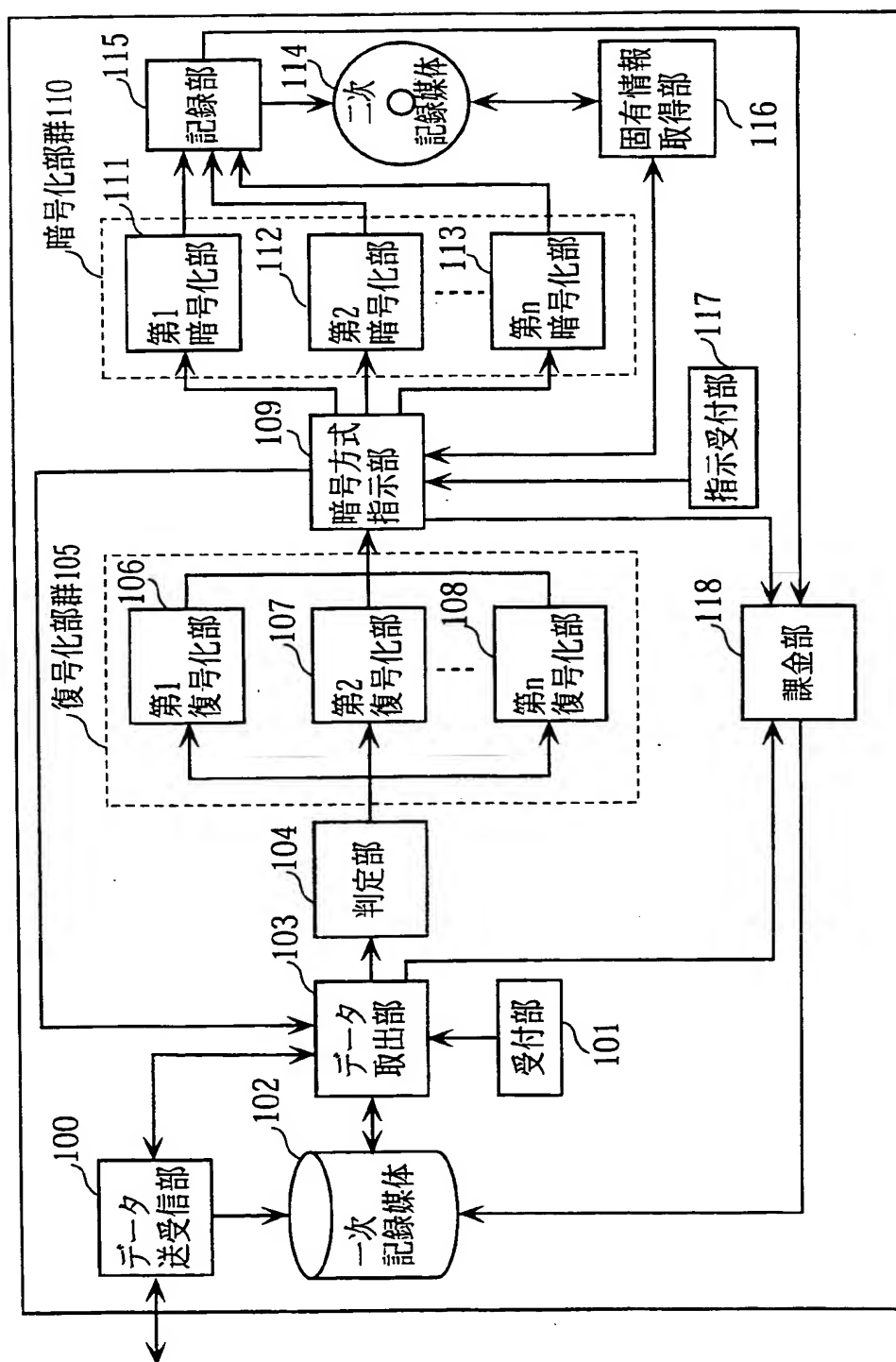
5 は当該データの暗号化方式を示す属性情報を含み、

複数の暗号化方式から一の暗号化方式を前記属性情報に基づいて判定する判定ステップを更に有し、

前記復号化ステップは、前記判定ステップに従い暗号化されたデジタルデータを復号化することをコンピュータに実行させるプログラムを記録した請求の範

10 囲第11項に記載のコンピュータ読み取り可能な記録媒体。

図1



デジタルデータ記録装置

図2

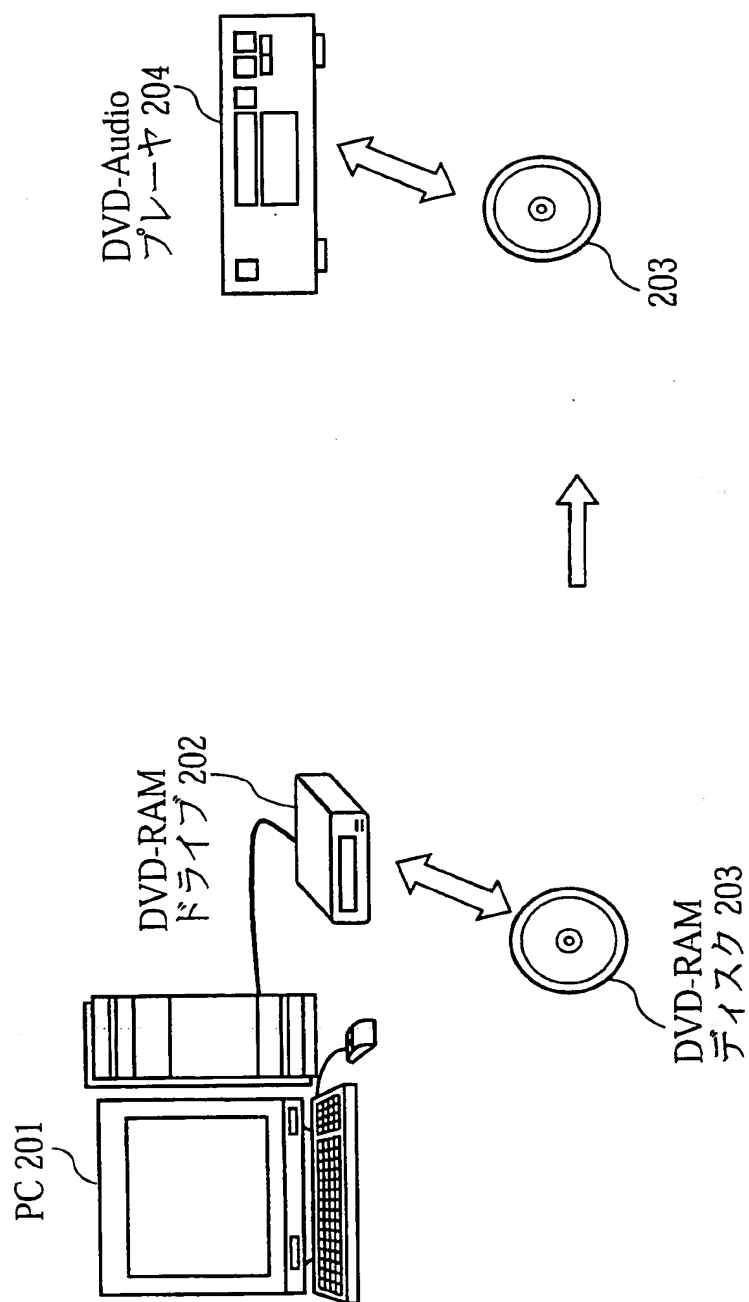


図3

301	302	303	304
曲名	歌手名	収録時間	価格
Song1	SingerA	4分20秒	100円
Song2	SingerB	3分53秒	50円
Song3	SingerC	4分48秒	75円
Song4	SingerD	4分06秒	100円
:	:	:	:
:	:	:	:

図4

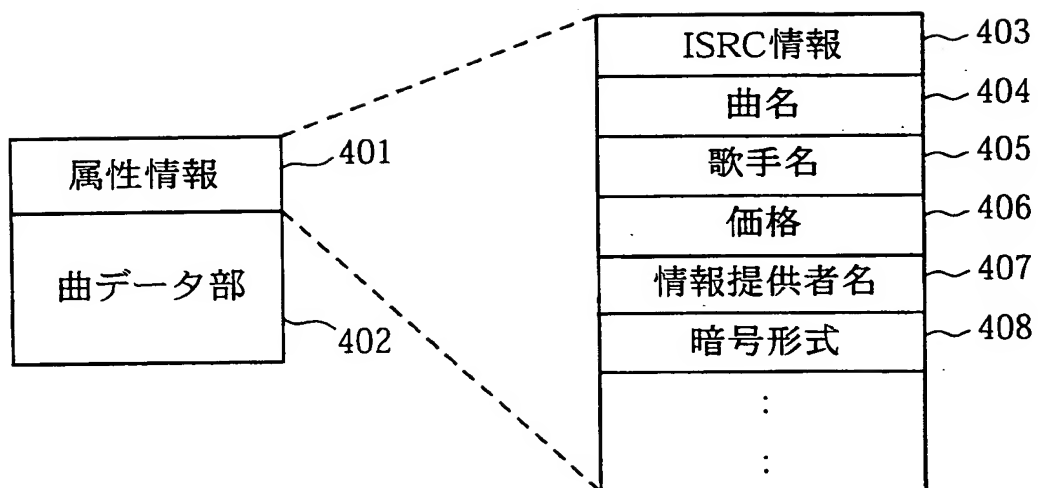


図5

301 曲名	302 歌手名	303 収録時間	501 価格(1)	502 価格(2)
Song1	SingerA	4分20秒	100円	70円
Song2	SingerB	3分53秒	50円	35円
Song3	SingerC	4分48秒	75円	50円
Song4	SingerD	4分06秒	100円	100円
:	:	:	:	:
:	:	:	:	:

図6

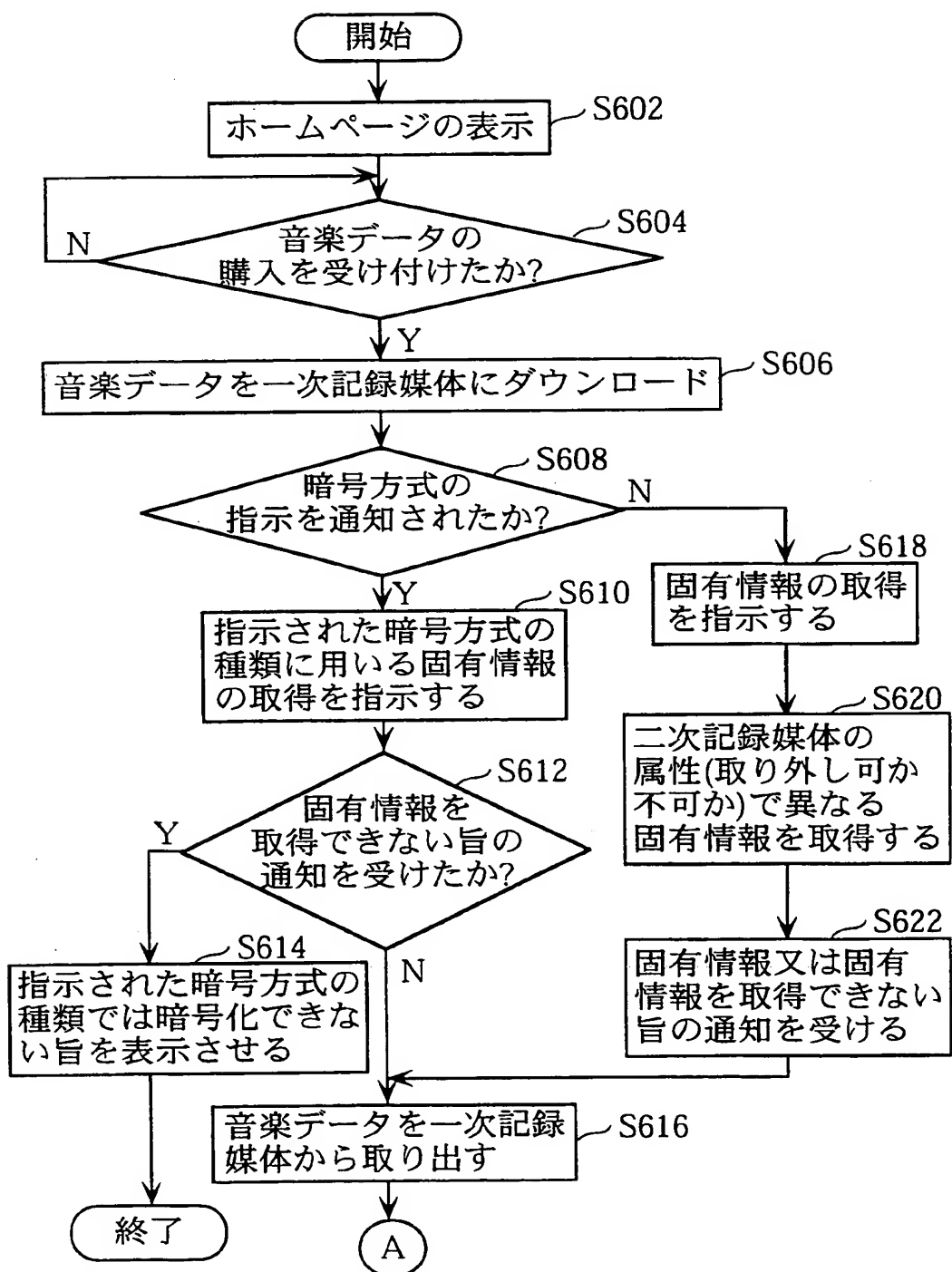


図7

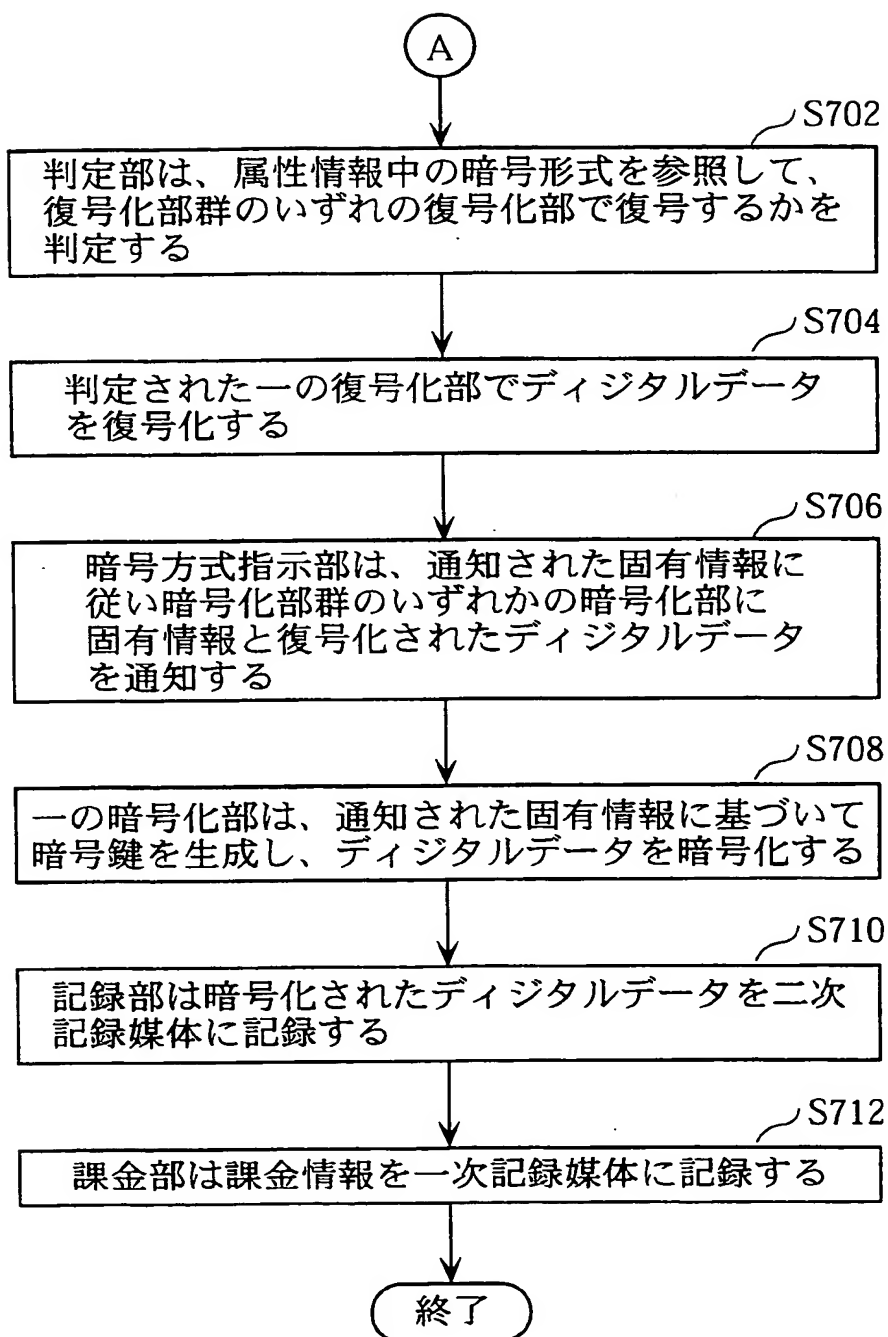


図8

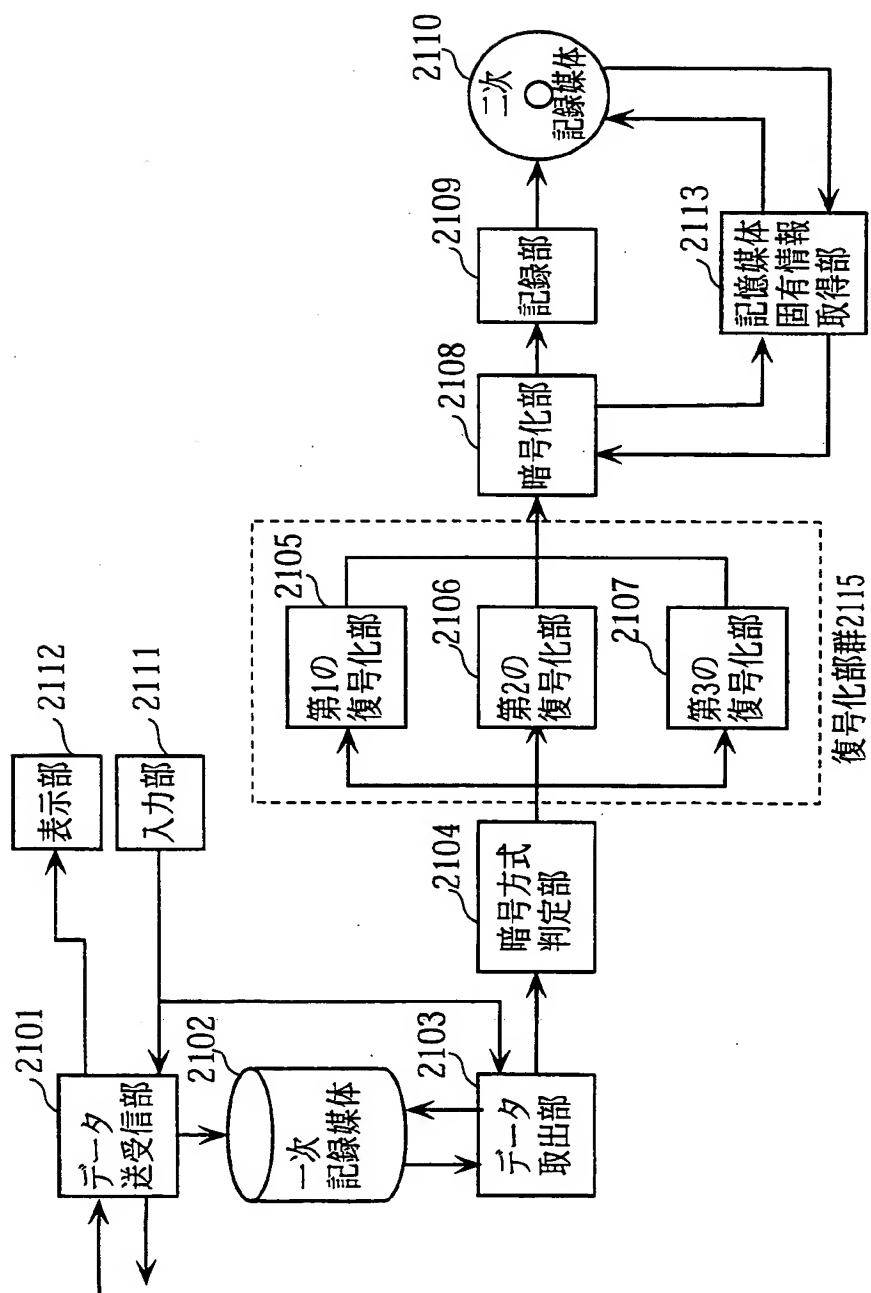


図9

2201		2202		2203		2204	
曲名	曲名コード	歌手名		データ入手先			
曲A	song01	A		www. song/song01			
曲B	song02	B		www. song/song02			
曲C	song03	C		www. song/song03			
曲D	song04	D		www. song/song04			
曲E	song05	E		www. song/song05			

図10

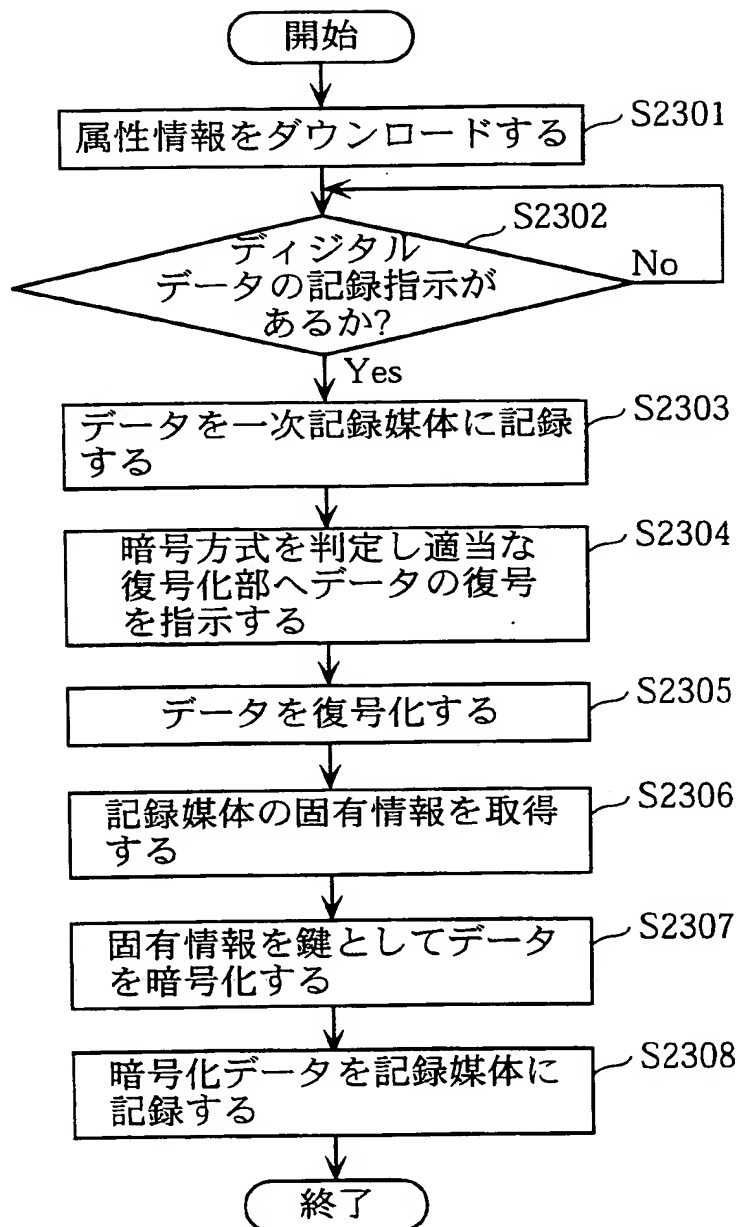


図11

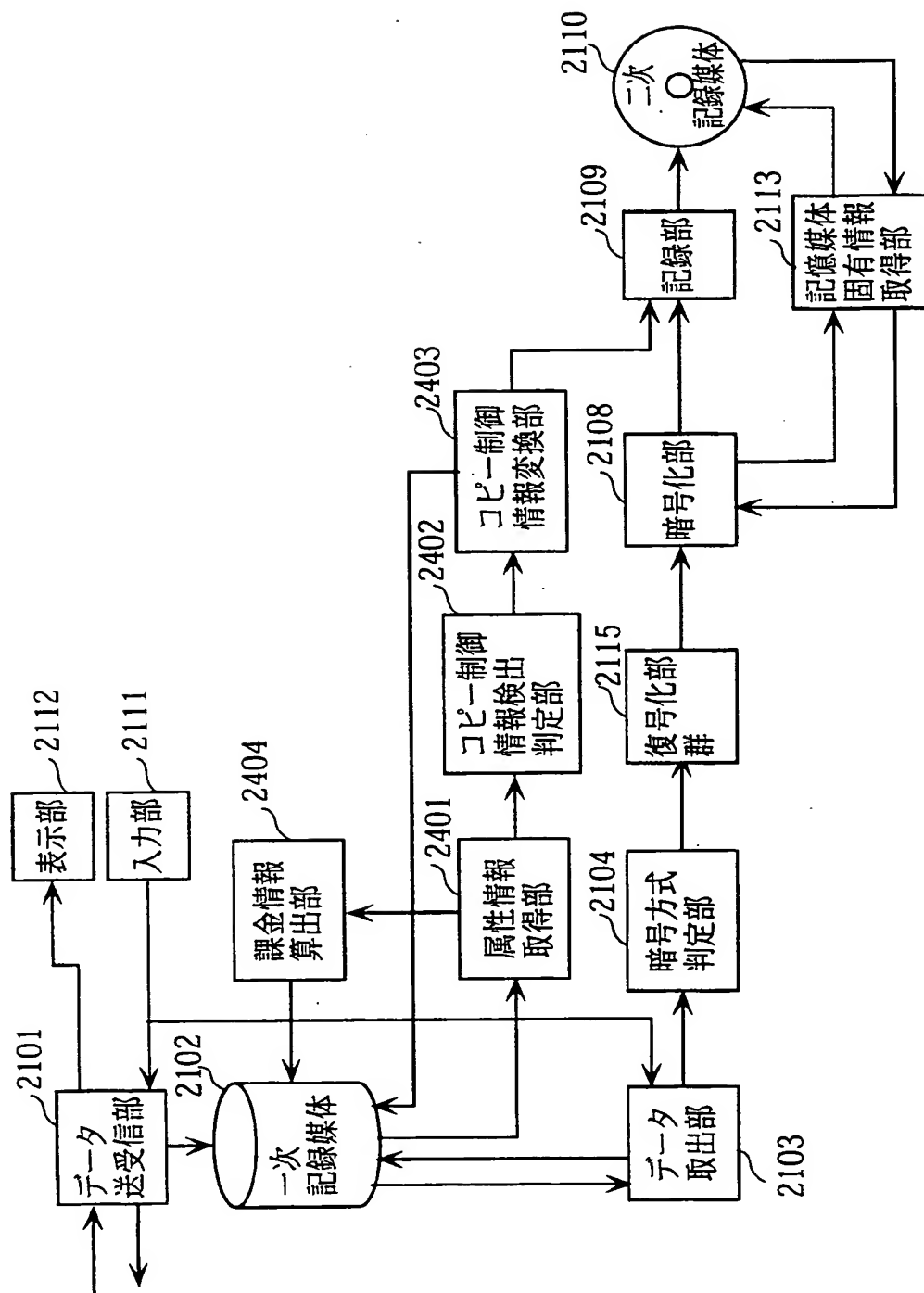


図12

2201 曲名	2202 曲名コード	2203 歌手名	2204 データ入手先	2501 コピー制御情報	2502 価格
曲A	song01	A	www. song/song01	孫コピー不可	100円
曲B	song02	B	www. song/song02	無制限に許可	10円
曲C	song03	C	www. song/song03	孫コピー不可	0円
曲D	song04	D	www. song/song04	孫コピー不可	30円
曲E	song05	E	www. song/song05	2回コピー可	10円

図13

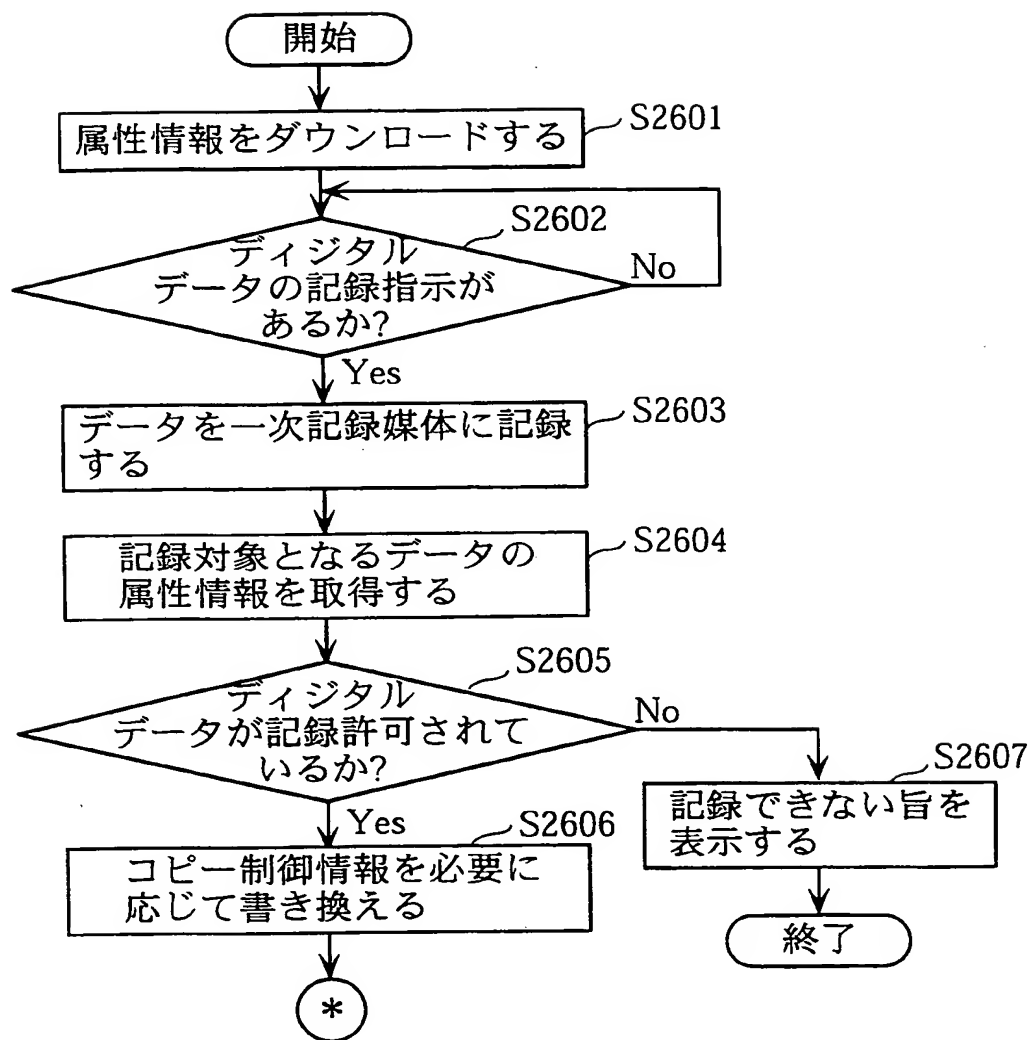


図14

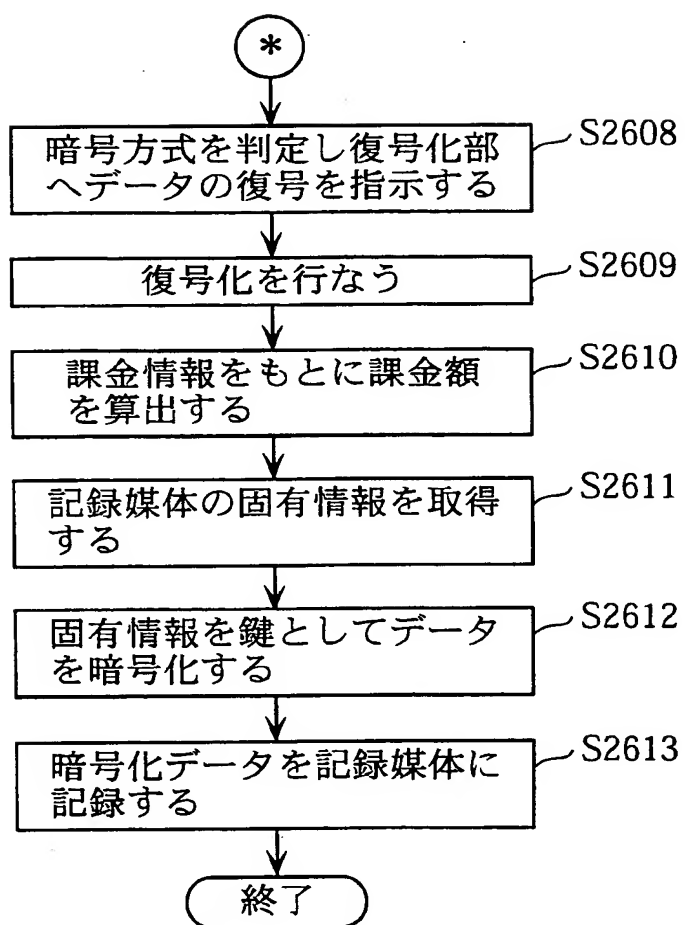


図 15

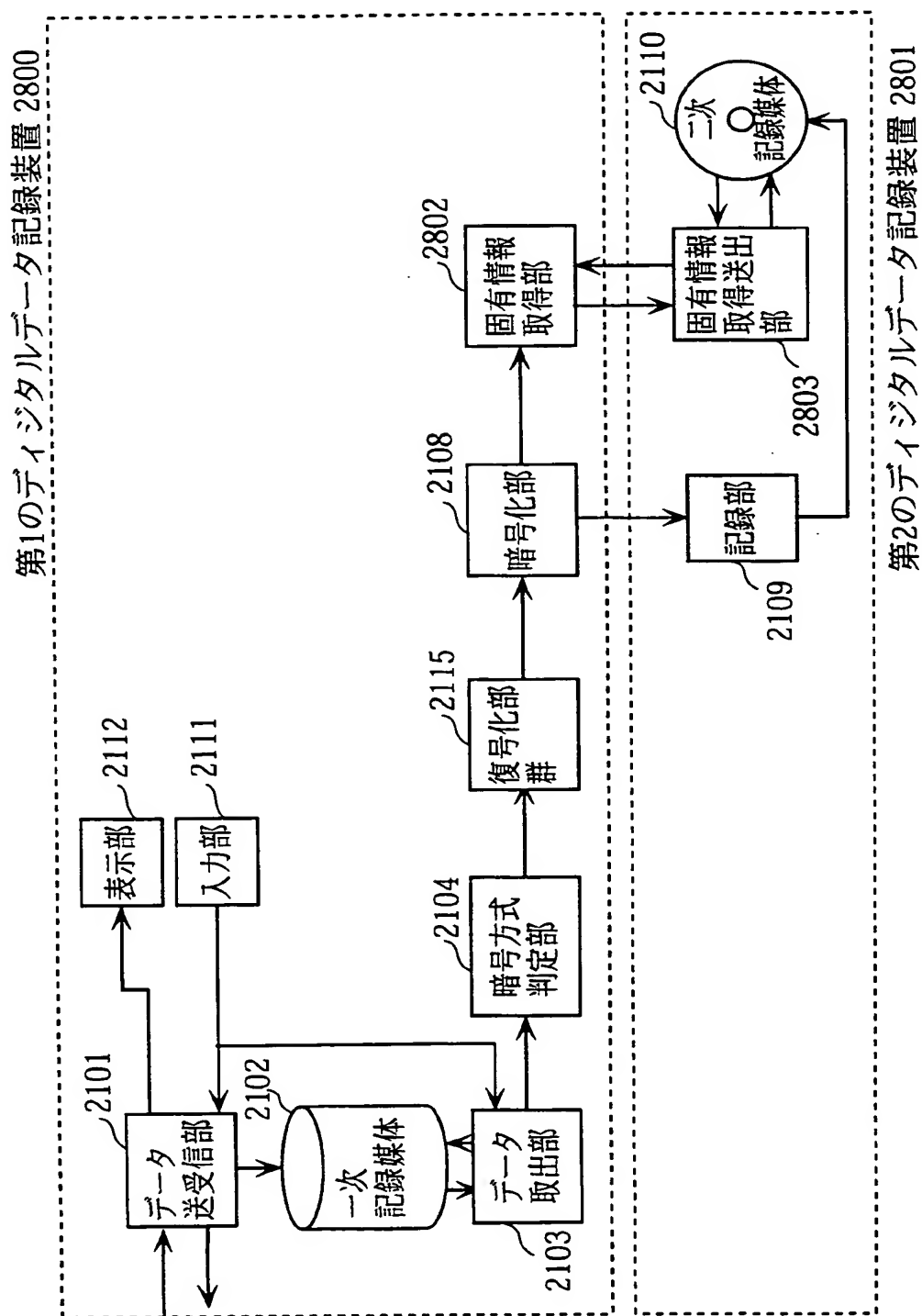


図16

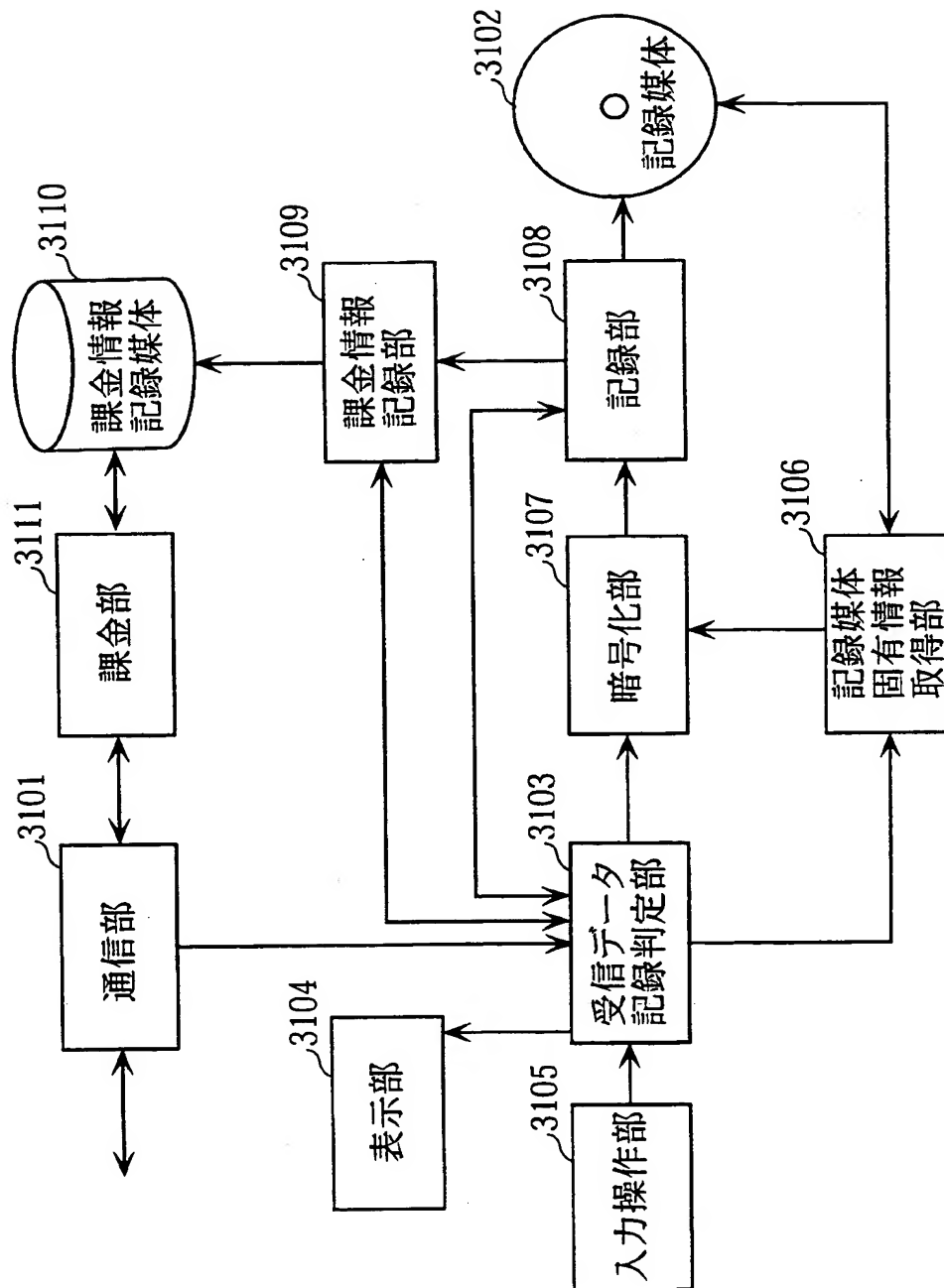


図17

属性情報 3201									
3202 3203		3204	3205		3206	3207	3208		3209
曲名	演奏者	曲名コード	記録料金	1回あたり再生料金	再生可能回数	暗号状態	コピー許可		
曲A	a	song01	100円	0.5円	100回	暗号あり	1回のみ可		
曲B	b	song02	10円	0円	無限	暗号なし	許可		
曲C	c	song03	0円	1円	50回	暗号あり	1回のみ可		
曲D	d	song04	30円	5円	50回	暗号あり	1回のみ可		
曲E	e	song05	10円	0円	10回	暗号なし	許可		
							...		

図18

管理情報 3301

曲名コード	記録開始 アドレス	記録終了 アドレス
song01	00320	00933
song02	14902	15172
song03	13085	13994
song04	50870	51825
song05	58349	58783

図19

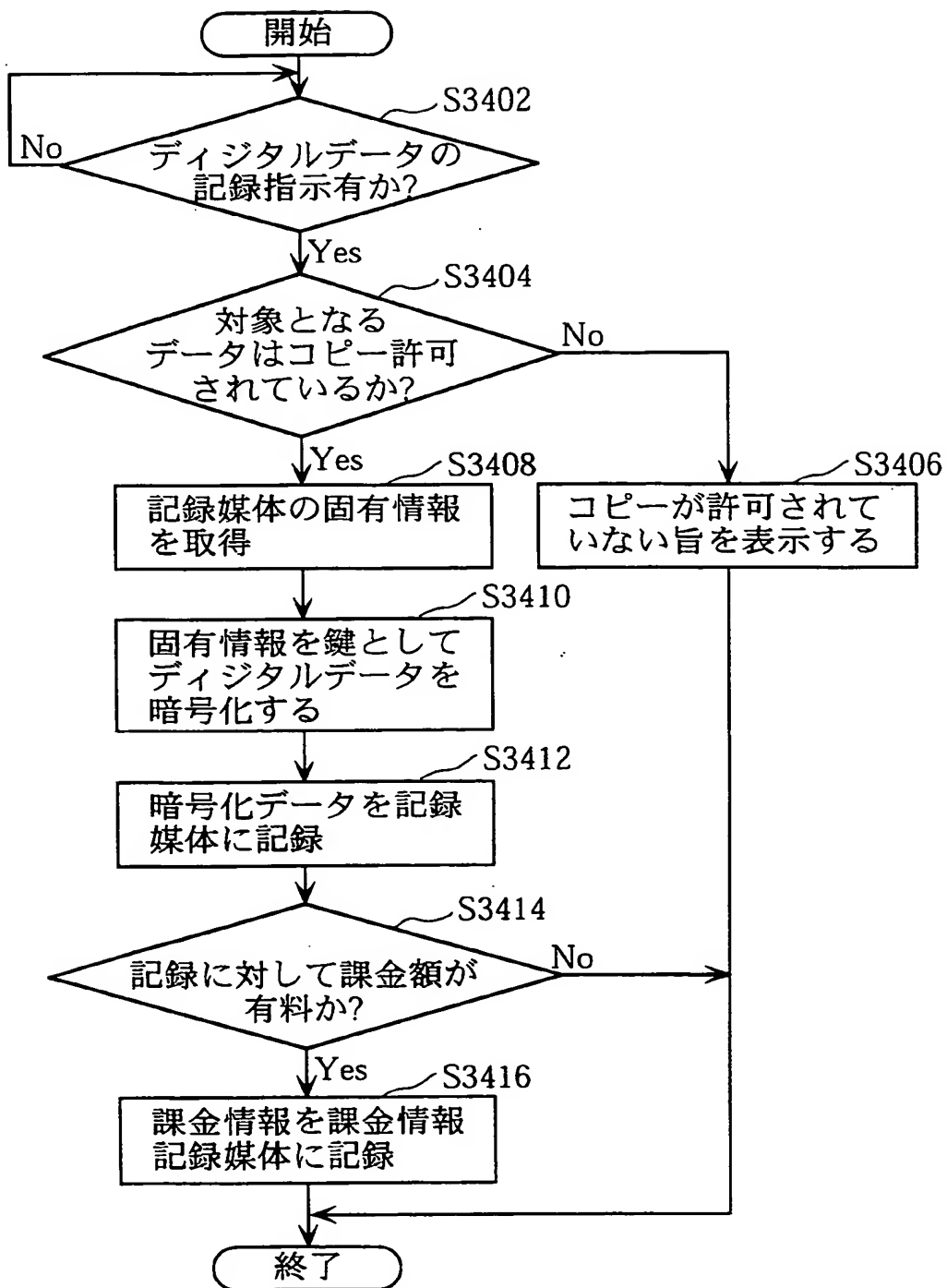


図20

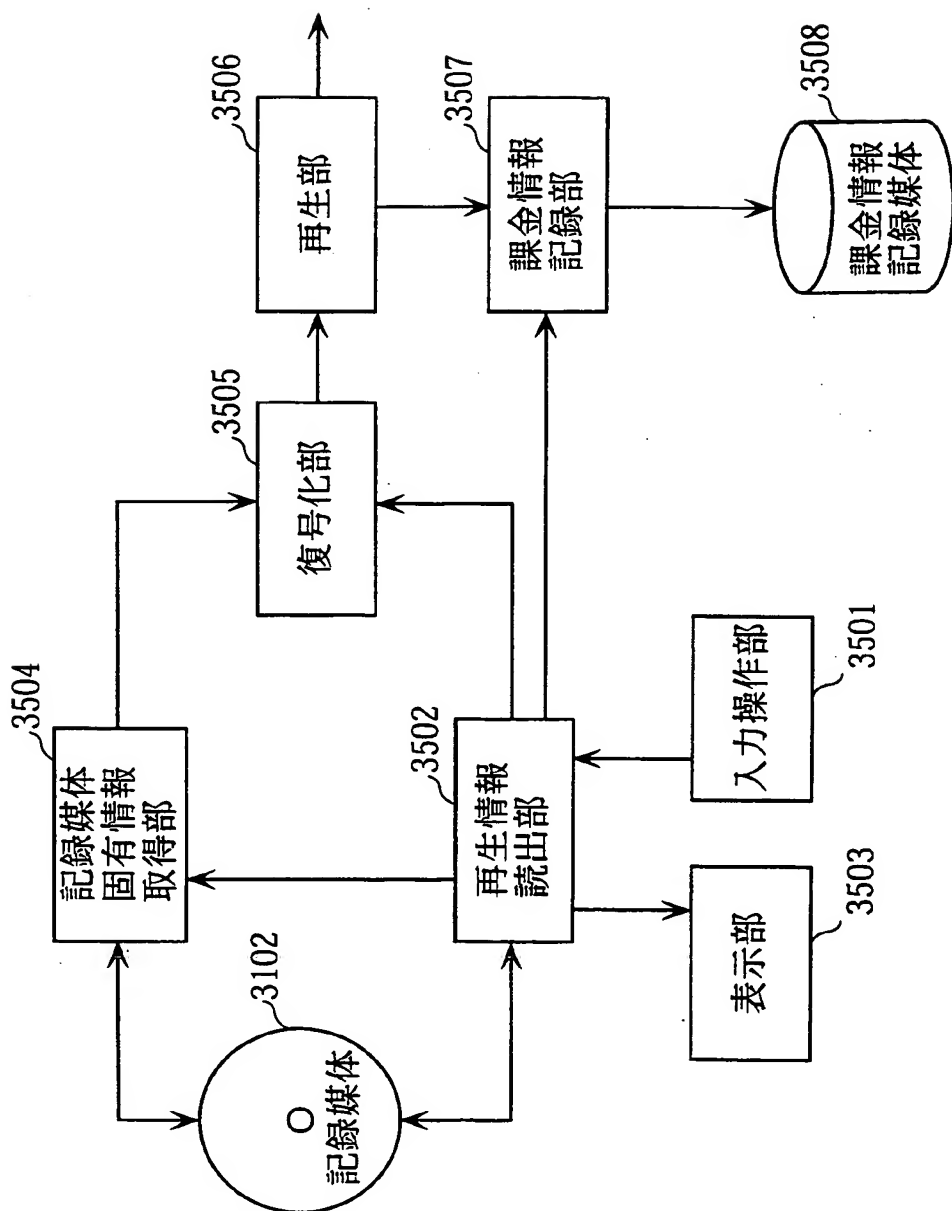


図21

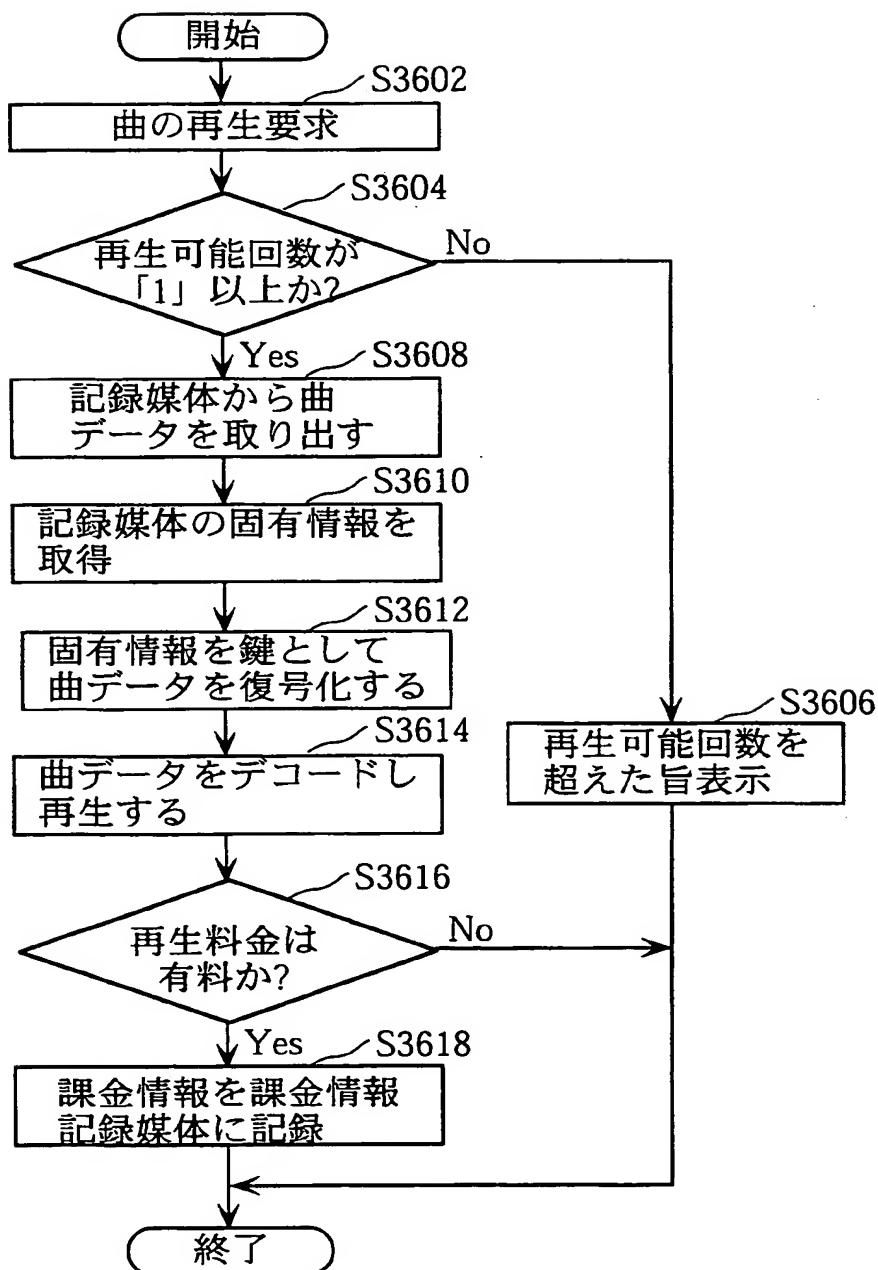


図22

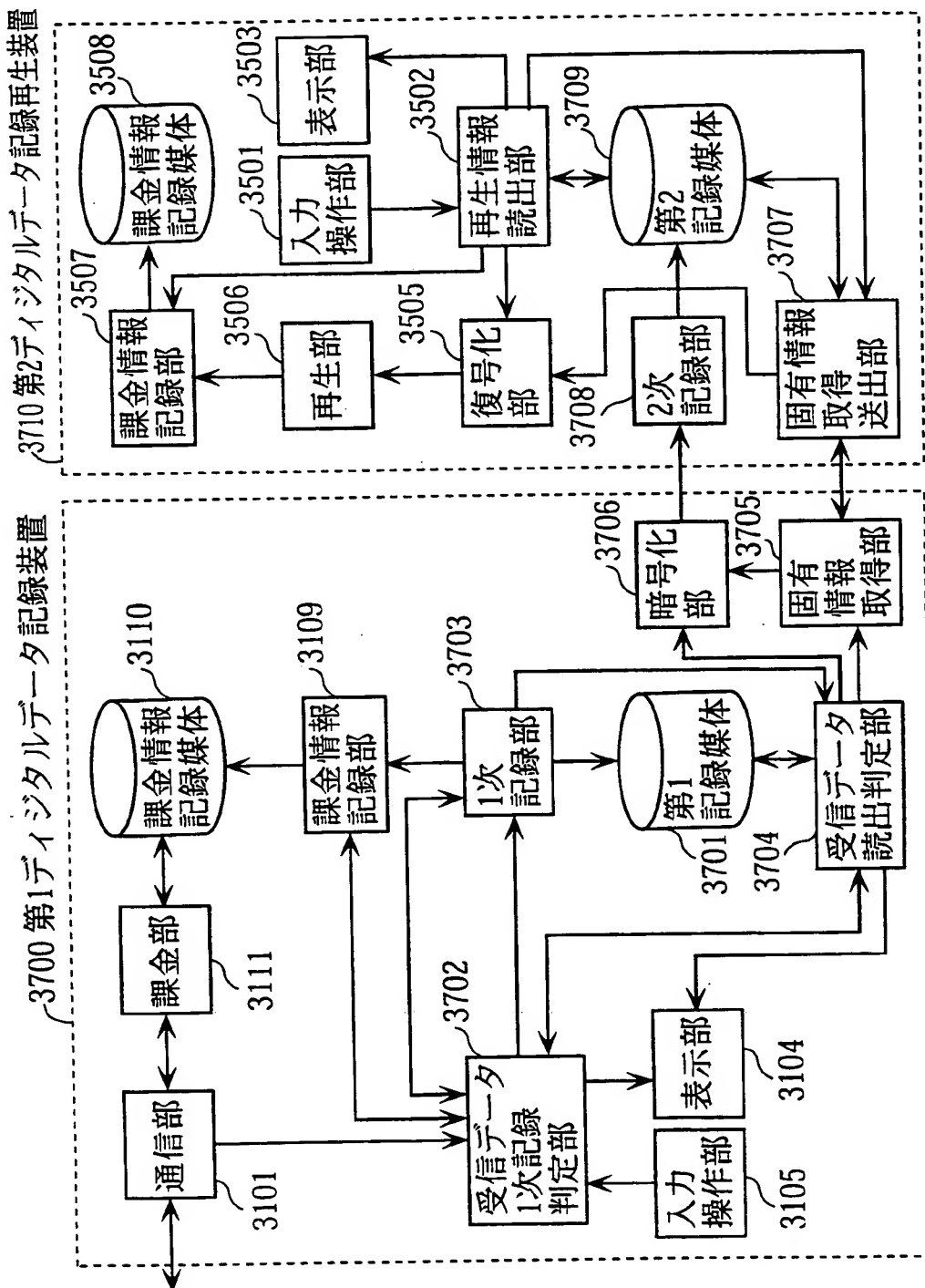


図23

属性情報 3801											
3805			3802			3803					3804
曲名	演奏者	曲名コード	1次記録料金	2次記録料金	1回あたり再生料金	再生可能回数	暗号状態	コピー許可(1次)	コピー許可(2次)	...	
曲A	a	song01	0円	100円	0.5円	100回	暗号あり	1回のみ可	1回のみ可	...	
曲B	b	song02	10円	10円	0円	無限	暗号なし	許可	許可	...	
曲C	c	song03	0円	0円	1円	50回	暗号あり	1回のみ可	1回のみ可	...	
曲D	d	song04	0円	30円	5円	50回	暗号あり	1回のみ可	1回のみ可	...	
曲E	e	song05	—	—	—	—	暗号なし	不許可	不許可	...	

図24

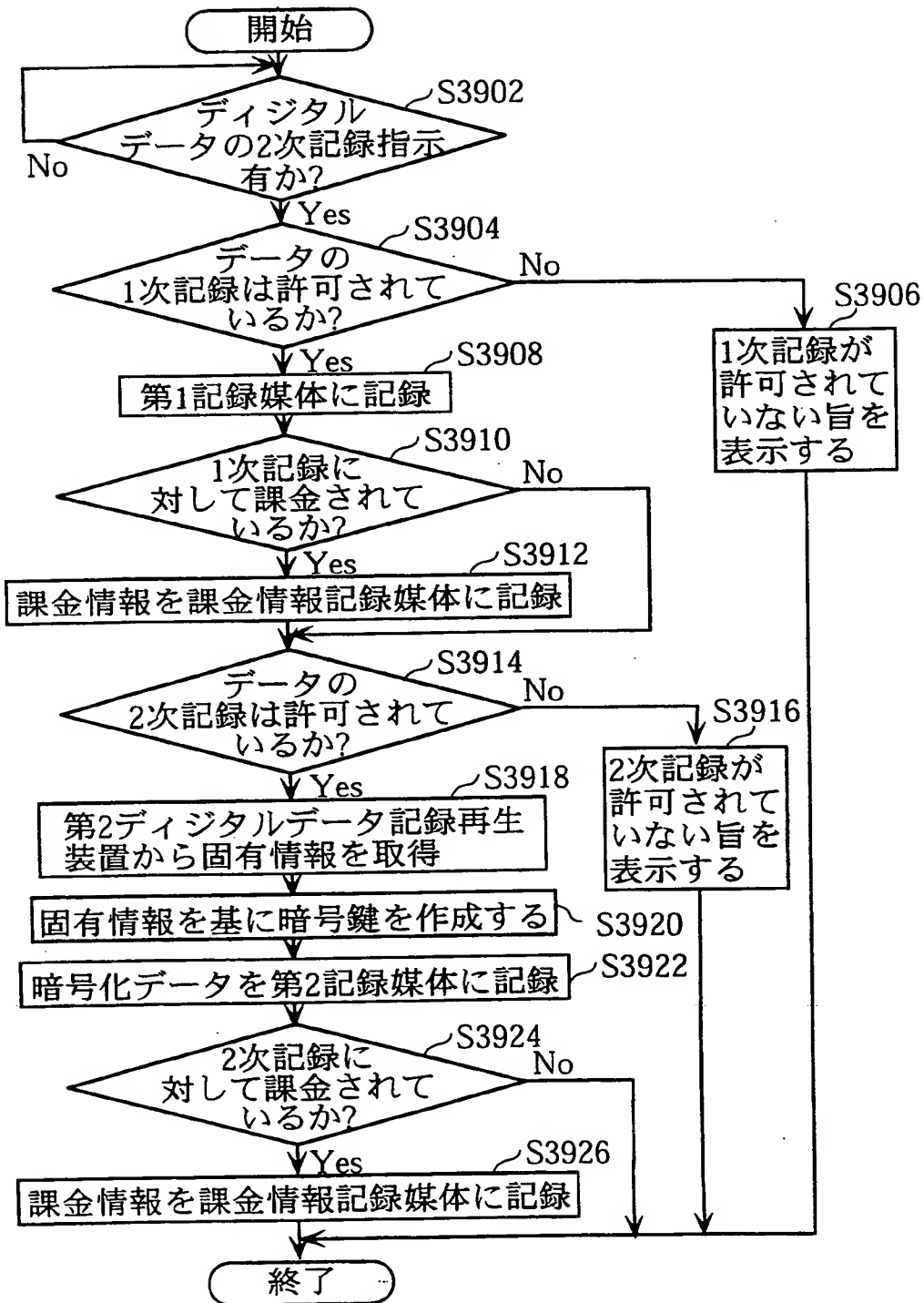


図25

...	曲名 コード	...	属性情報31001				...
			31003	31002	31004	31005	
...	2次記録料金				...
			媒体ID	機器ID	媒体ID+機器ID		
...	song01	...	100円	10円	10円	10円	...
...	song02	...	10円	1円	1円	1円	...
...	song03	...	0円	0円	0円	0円	...
...	song04	...	30円	3円	3円	3円	...
...	song05	...	10円	1円	1円	1円	...

INTERNATIONAL SEARCH REPORT

International application No.

PCT/JP99/03887

A. CLASSIFICATION OF SUBJECT MATTER

Int.Cl⁶ G11B20/10

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Int.Cl⁶ G11B20/10

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Jitsuyo Shinan Koho 1922-1999 Toroku Jitsuyo Shinan Koho 1994-1999

Kokai Jitsuyo Shinan Koho 1971-1999 Jitsuyo Shinan Toroku Koho 1996-1999

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP, 7-272399, A (Hitachi, Ltd.), 20 October, 1995 (20. 10. 95), Full text ; Figs. 1 to 18 & US, 5912969, A	1-12
A	JP, 8-339629, A (Matsushita Electric Industrial Co., Ltd.), 24 December, 1996 (24. 12. 96), Full text ; Figs. 1 to 4 (Family: none)	1-12
P, A	JP, 11-191266, A (Kobe Steel, Ltd.), 13 July, 1999 (13. 07. 99), Full text ; Figs. 1, 2 (Family: none)	1-12

☐ Further documents are listed in the continuation of Box C.

☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search
19 October, 1999 (19. 10. 99)

Date of mailing of the international search report
2 November, 1999 (02. 11. 99)

Name and mailing address of the ISA/
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

A. 発明の属する分野の分類 (国際特許分類 (IPC))
Int. Cl.⁶ G11B20/10

B. 調査を行った分野

調査を行った最小限資料 (国際特許分類 (IPC))
Int. Cl.⁶ G11B20/10

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	1922-1999年
日本国公開実用新案公報	1971-1999年
日本国登録実用新案公報	1994-1999年
日本国実用新案登録公報	1996-1999年

国際調査で使用した電子データベース (データベースの名称、調査に使用した用語)

C. 関連すると認められる文献

引用文献の カテゴリー*	引用文献名 及び一部の箇所が関連するときは、その関連する箇所の表示	関連する 請求の範囲の番号
A	JP, 7-272399, A (株式会社日立製作所) 20. 10月. 1995 (20. 10. 95) 全文, 第1-18図 & US, 5912969, A	1-12
A	JP, 8-339629, A (松下電器産業株式会社) 24. 12月. 1996 (24. 12. 96) 全文, 第1-4図 (ファミリーなし)	1-12
P, A	JP, 11-191266, A (株式会社神戸製鋼所) 13. 7月. 1999 (13. 07. 99) 全文, 第1-2図 (ファミリーなし)	1-12

☐ C欄の続きにも文献が列挙されている。

☐ パテントファミリーに関する別紙を参照。

* 引用文献のカテゴリー

「A」特に関連のある文献ではなく、一般的技術水準を示すもの

「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの

「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献 (理由を付す)

「O」口頭による開示、使用、展示等に言及する文献

「P」国際出願日前で、かつ優先権の主張の基礎となる出願

の日の後に公表された文献

「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの

「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの

「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの

「&」同一パテントファミリー文献

国際調査を完了した日

19. 10. 99

国際調査報告の発送日

02.11.99

国際調査機関の名称及びあて先

日本国特許庁 (ISA/JP)

郵便番号100-8915

東京都千代田区霞が関三丁目4番3号

特許庁審査官 (権限のある職員)

小松 正

5Q

7736

電話番号 03-3581-1101 内線 6922

50791336 W000

(12) **EUROPEAN PATENT APPLICATION**
 published in accordance with Art. 158(3) EPC

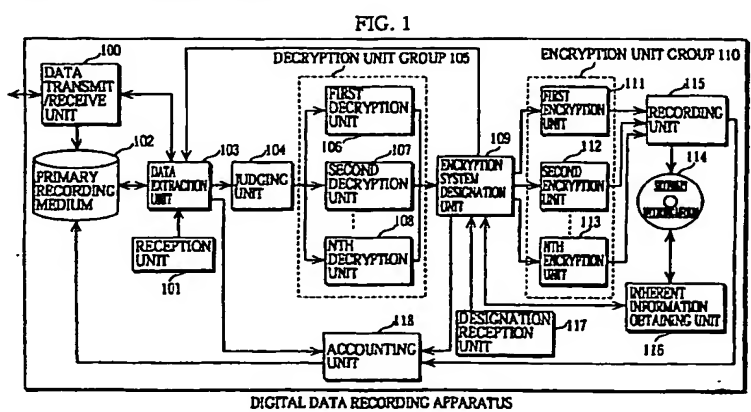
(43) Date of publication: 12.07.2000 Bulletin 2000/28
 (21) Application number: 99931449.5
 (22) Date of filing: 21.07.1999
 (51) Int. Cl.⁷: **G11B 20/10**
 (86) International application number: PCT/JP99/03887
 (87) International publication number: WO 00/05716 (03.02.2000 Gazette 2000/05)

<p>(84) Designated Contracting States: DE FR GB IT NL</p> <p>(30) Priority: 22.07.1998 JP 20696798 12.10.1998 JP 28983198</p> <p>(71) Applicant: Matsushita Electronics Corporation Kadoma-shi, Osaka 571-8501 (JP)</p> <p>(72) Inventors: • TAGAWA, Kenji Katano-shi, Osaka 576-0021 (JP)</p>	<p>• MINAMI, Masataka Tsuna-gun, Hyogo 656-2311 (JP)</p> <p>• KOZUKA, Masayuki Neyagawa-shi, Osaka 572-0024 (JP)</p> <p>(74) Representative: Crawford, Andrew Birkby et al A.A. Thornton & Co. 235 High Holborn London WC1V 7LE (GB)</p>
--	--

(54) **DIGITAL DATA RECORDING DEVICE AND METHOD FOR PROTECTING COPYRIGHT AND EASILY REPRODUCING ENCRYPTED DIGITAL DATA AND COMPUTER READABLE RECORDING MEDIUM RECORDING PROGRAM**

(57) A data transmit/receive unit receives encrypted digital data distributed through an electronic music distribution system and records the digital data on a primary recording medium. Digital data have been encrypted in different encryption systems according to the distributors, and include attribute information indicating the encryption systems. The encryption system of digital data that has been extracted by a data extraction unit is judged by a judging unit and decrypted by an appropriate decryption unit. An inherent information obtaining unit obtains the identification information of a secondary recording medium or a playback apparatus

according to whether the secondary recording medium can be removable from the playback apparatus. An encryption system designation unit selects one out of a plurality of encryption units according to the obtained identification information. The selected encryption unit creates an encryption key according to the identification information and encrypts the digital data. A recording unit records the digital data on the secondary recording medium. An accounting unit charges according to accounting information in the attribute information.



EP 1 018 733 A1

Description

FIELD OF THE INVENTION

[0001] The present invention relates to a digital data recording apparatus, a digital data recording method, and a computer-readable recording medium for protecting copyrights of digital data.

BACKGROUND OF THE INVENTION

[0002] Thanks to the recent widespread use of the Internet, distribution of music with so-called EC (Electronic Commerce) has been developed, in which desired music data is downloaded from a homepage using a PC (Personal Computer) and the bill is charged to a credit card, for instance. The widespread of the music distribution through the Internet using the EC (referred to "electronic music distribution" in this specification) would reduce the necessity for consumers to go to record shops and might drastically change the distribution of music, which has been mainly distributed by CDs (Compact Discs).

[0003] Meanwhile, many people listen to music not only at home but also on their way to office, school, home, and in a car using a portable playback apparatus and the like. In these cases, music data must be recorded on a portable medium such as an MD (Mini Disc).

[0004] Regarding electronic music distribution, delivery companies adopt a variety of encryption systems to protect copyrights. More specifically, a different optimum encryption system is adopted according to the manufacturing company, the distribution route, the usage pattern, and the like. Under the circumstances, when music data that has been distributed through an electronic music distribution system is recorded on an MD, the playback apparatus is required to decode the music data on the MD according to the adopted encryption method. As a result, the playback apparatus is bulky, expensive, and not useful for users.

[0005] It is useful for users when music data that has been distributed through an electronic music distribution system is decoded at the time of recording on an MD since playback apparatuses can be inexpensive.

[0006] In this case, however, unauthorized duplication of music data is encouraged, so that the copyright of music data cannot be fully protected.

DISCLOSURE OF THE INVENTION

[0007] It is accordingly an object of the present invention to provide a digital data recording apparatus, a digital data recording method, and a computer-readable recording medium for protecting copyrights and reproducing music data recorded on a recording medium with an inexpensive digital data playback apparatus.

[0008] The above-mentioned object may be

achieved by a digital data recording apparatus for recording digital data on a recording medium that may include: a communication unit for receiving encrypted digital data via a digital network; a decryption unit for decrypting the encrypted digital data that has been received by the communication unit; an encryption unit including a plurality of encryption sub-units that re-encrypt decrypted digital data in encryption systems having different security levels; a recording unit for recording digital data that has been re-encrypted by the encryption unit on the recording medium; and a controller for controlling the decryption unit and the encryption unit, wherein the controller has one of the plurality of encryption sub-units re-encrypt the digital data that has been decrypted by the decryption unit.

[0009] As a result, it is possible to record digital data that has been re-encrypted by the encryption unit and can be easily reproduced by the playback apparatus. It is also possible to protect the copyright since the digital data has been re-encrypted.

[0010] The above-mentioned object may be also achieved by the digital data recording apparatus, wherein the digital data that has been recorded on the recording medium is reproduced by a playback apparatus, the encryption unit includes: a first encryption sub-unit for re-encrypting digital data using an encryption key that has been created according to identification information of the recording medium; and a second encryption sub-unit for re-encrypting digital data using an encryption key that has been created according to identification information of the playback apparatus; and the controller judges whether the recording medium is removable from the playback apparatus, has the first encryption sub-unit re-encrypt the decrypted digital data when the recording medium is removable from the playback apparatus, and has the second encryption sub-unit re-encrypt the decrypted digital data when the recording medium is not removable from the playback apparatus.

[0011] As a result, when digital data on a recording medium is reproduced by a playback apparatus, the digital data may be reproduced by re-encrypting the digital data using an encryption key that has been created according to the identification information of the recording medium. On the other hand, when digital data on a recording medium is reproduced by a specific playback apparatus, the digital data may be reproduced by the specific playback apparatus by re-encrypting the digital data using an encryption key that has been created according to the identification information of the specific playback apparatus.

[0012] The above-mentioned object may be also achieved by the digital data recording apparatus that may include an accounting unit for conducting an accounting process via the digital network, wherein the controller determines an accounting value according to an encryption sub-unit that has re-encrypted the decrypted digital data, and controls the accounting unit

so that the controller conducts the accounting process according to the determined accounting value.

[0013] As a result, it is possible to select one of the plurality of encryption sub-units that re-encrypt digital data in encryption systems having different security levels and to pay a charge according to the selected encryption sub-unit.

[0014] The above-mentioned object may be also achieved by the digital data recording apparatus, wherein the controller prohibits the decryption unit from decrypting the encrypted digital data when the encryption unit fails to create any encryption key.

[0015] As a result, unnecessary decryption of digital data may be prevented when the encryption unit fails to create any encryption key.

[0016] The above-mentioned object may be also achieved by the digital data recording apparatus, wherein the security levels of the encryption systems in which the plurality of encryption sub-units re-encrypt decrypted digital data are lower than security levels of encryption systems in which encrypted digital data that are to be received by the communication unit have been encrypted.

[0017] As a result, a playback apparatus may easily reproduce digital data, leading to a less expensive playback apparatus.

[0018] The above-mentioned object may be also achieved by the digital data recording apparatus, wherein the encrypted digital data that is received by the communication unit has been encrypted in one of encryption systems having different security levels and includes attribute information that indicates the encryption system, the decryption unit includes a plurality of decryption sub-units that decrypt encrypted digital data that have been encrypted in the encryption systems, and the controller judges the encryption system in which the encrypted digital data has been encrypted according to the attribute information, and controls the decryption unit so that one of the plurality of decryption sub-units corresponding to the judged encryption system decrypts the encrypted digital data.

[0019] As a result, even when received digital data have been encrypted in encryption systems having different security levels, it is possible to decrypt digital data by selecting a decryption sub-unit according to the encryption system in which the digital data has been encrypted.

[0020] The above-mentioned object may be also achieved by the digital data recording apparatus that may further include an accounting unit for conducting an accounting process via the digital network, wherein the controller determines an accounting value according to a decryption sub-unit that has decrypted the encrypted digital data and an encryption sub-unit that has re-encrypted the decrypted digital data, and controls the accounting unit so that the controller conducts the accounting process according to the determined accounting value.

[0021] As a result, it is possible to pay a charge according to the decryption and re-encryption of digital data and to protect the copyright.

[0022] The above-mentioned object may be also achieved by a digital data recording method of recording digital data on a recording medium, the digital data recording method may include: a communication step for receiving encrypted digital data via a digital network; a decryption step for decrypting the encrypted digital data that has been received at the communication step; an encryption step for re-encrypting decrypted digital data in one of a plurality of encryption systems having different security levels; and a recording step for recording digital data that has been re-encrypted at the encryption step on the recording medium.

[0023] As a result, it is possible to record digital data on a recording medium that has been re-encrypted in an encryption system so that the digital data is easily reproduced by a playback apparatus. In addition, since the digital data is re-encrypted, the copyright may be protected.

[0024] The above-mentioned object may be also achieved by the digital data recording method, wherein the encrypted digital data that is received at the communication step has been encrypted in one of encryption systems having different security levels and includes attribute information that indicates the encryption system, the digital data recording method, further comprising a judging step for judging one of the plurality of encryption systems according to the attribute information, wherein the decryption step decrypts the encrypted digital data according to the judgement at the judging step.

[0025] As a result, digital data that has been recorded on a recording medium may be reproduced by any playback apparatus or only by a specific playback apparatus.

[0026] The above-mentioned object may be also achieved by a computer-readable recording medium that is applied to a digital data recording apparatus for recording digital data on a first recording medium, the computer-readable recording medium storing a program that has a computer execute steps: a communication step for receiving encrypted digital data via a digital network; a decryption step for decrypting the encrypted digital data that has been received at the communication step; an encryption step for re-encrypting decrypted digital data in one of a plurality of encryption systems having different security levels; and a recording step for recording digital data that has been re-encrypted at the encryption step on the recording medium.

[0027] As a result, it is possible to record digital data on a recording medium that has been re-encrypted in an encryption system so that the digital data is easily reproduced by a playback apparatus. In addition, it is possible to protect copyrights by using the recording medium in a digital data recording apparatus that has no function to protect copyrights.

[0028] The above-mentioned object may be also achieved by the computer-readable recording medium, wherein the encrypted digital data that is received at the communication step has been encrypted in one of encryption systems having different security levels and includes attribute information that indicates the encryption system, the digital data recording method may further include a judging step for judging one of the plurality of encryption systems according to the attribute information, wherein the decryption step decrypts the encrypted digital data according to the judgement at the judging step.

[0029] As a result, it is possible to reproduce digital data that has been recorded on the first recording medium by any playback apparatus or by a specific apparatus.

BRIEF DESCRIPTION OF THE DRAWINGS

[0030] These and other objects, advantages and features of the invention will become apparent from the following description thereof taken in conjunction with the accompanying drawings that illustrate a specific embodiment of the invention. In the Drawings:

Fig. 1 shows the structure of a digital data recording apparatus according to the first embodiment of the present invention;

Fig. 2 is an external view of the hardware configuration of the first embodiment of the present invention and an external view of a playback apparatus of a recording medium according to the first embodiment of the present invention;

Fig. 3 shows an example of a display screen of a home page for purchasing music data according to the first embodiment of the present invention;

Fig. 4 shows an example of data structure of music data downloaded on a primary recording medium according to the first embodiment of the present invention;

Fig. 5 shows an example of a display screen of a home page for purchasing music data according to the first embodiment of the present invention;

Fig. 6 is a first flowchart illustrating the operations in the first embodiment of the present invention;

Fig. 7 is a second flowchart illustrating the operations in the first embodiment of the present invention;

Fig. 8 shows the structure of a digital data recording apparatus according to the second embodiment of the present invention;

Fig. 9 is an example of information that is displayed on a display unit when digital signals provided by the information provider are recorded in the second embodiment;

Fig. 10 is a flowchart showing the operations in the second embodiment;

Fig. 11 shows the structure of a digital data record-

ing apparatus according to the third embodiment of the present invention;

Fig. 12 shows the attribute information of data in the third embodiment;

Fig. 13 is a flowchart showing operations in the third embodiment;

Fig. 14 is a flowchart showing operations in the third embodiment;

Fig. 15 shows the structure of the digital data recording apparatus according to the fourth embodiment of the present invention;

Fig. 16 shows the structure of a digital data recording apparatus according to the sixth embodiment of the present invention;

Fig. 17 is an example of attribute information;

Fig. 18 shows an example of management information;

Fig. 19 is a flowchart showing operations in the sixth embodiment;

Fig. 20 shows the structure of a playback apparatus for reproducing digital data that has been recorded in the sixth embodiment;

Fig. 21 is a flowchart showing operation by the digital data playback apparatus in the sixth embodiment;

Fig. 22 shows the structure of a digital data recording apparatus according to the seventh embodiment of the present invention;

Fig. 23 shows an example of the data structure of attribute information that is attached to digital data when transmitted in seventh embodiment;

Fig. 24 is a flowchart showing operations in seventh embodiment;

Fig. 25 shows an example of the data structure of attribute information that is attached to digital data when transmitted in another example of seventh embodiment.

DESCRIPTION OF THE PREFERRED EMBODIMENTS

[0031] An explanation of the preferred embodiments of a digital data recording apparatus according to the present invention will be given with reference to figures.

(The First Embodiment)

[0032] Fig. 1 shows the structure of a digital data recording apparatus according to the first embodiment of the present invention. The digital data recording apparatus includes a data transmit/receive unit 100, a reception unit 101, a primary recording medium 102, a data extraction unit 103, a judging unit 104, a decryption unit group 105, an encryption system designation unit 109, an encryption unit group 110, a secondary recording medium 114, a recording unit 115, an inherent information obtaining unit 116, a designation reception unit

117, and an accounting unit 118.

[0033] Note that each element of the digital data recoding apparatus apart from the secondary recording medium 114 and the recording unit 115 is generally realized by a PC (Personal Computer) 201 as shown in Fig. 2. The recording unit 115 is realized by, for instance, a DVD (Digital Versatile Disc) -RAM drive 202, and the secondary recording medium 114 is realized by a DVD-RAM disc 203.

[0034] The digital data recording apparatus receives music data, i.e., encrypted digital data that is distributed through the Internet, and downloads the received music data on the primary recording medium 102. Then the digital data recording apparatus decodes the digital data in the decryption unit group 105, re-encrypts the decoded digital data in the encryption unit group 110, and records the re-encrypted digital data in the secondary recording medium.

[0035] Note that although an explanation of electronic music distribution will be given in the present embodiment, the kind of distributed digital data is not limited to music. Distributed digital data may be video data, character data, or the combination of those kinds of data.

[0036] The data transmit/receive unit 100 is a communication unit realized by a modem and a control software, and is connected to the host computer (not illustrated) of the information provider through a telephone line. When informed of the purchase requirement of a piece of music that has been received by the reception unit 101 via the data extraction unit 103, the data transmit/receive unit 100 transmits the purchase requirement to the host computer. The data transmit/receive unit 100 downloads music data from the host computer according to the purchase requirement via the Internet and records the downloaded music data on the primary recording medium. Meanwhile, the data transmit/receive unit 100 transmits accounting information to the host computer that has been generated at the time of the purchase of music.

[0037] Here, an explanation of information provided by the information provider will be given. The information provider sets up a site, i.e., a homepage for the sale of music data to provide information such as music titles and prices that are necessary for users to purchase music data and may arouse the interest of users. Users purchase desired music data according to the information provided by the information provider.

[0038] Fig. 3 shows an example of homepage for the sale of music data provided by an information provider. The information includes titles 301, singers 302, times 303, and prices 304. A title 301 and a singer 302 show the title and singer of one piece of music data. A time 303 shows the time required to record (play back) one piece of music data, and a price 304 shows the selling price of one piece of music data. A user selects a piece of music according to the information and informs the data transmit/receive unit 100 of purchase require-

ment through the reception unit 101. Needless to say, the information provided by the information provider is not limited to character information as shown in Fig. 3. The information may be images such as jacket pictures and music data for test-listening.

[0039] The reception unit 101 includes a keyboard and a mouse, and receives purchase requirement from the user who has watched the information shown in Fig. 3 on the display screen of the PC. The received purchase requirement is transferred to the data transmit/receive unit 100 via the data extraction unit 103.

[0040] The primary recording medium 102 is realized by a hard disk in the PC, and stores the music data, i.e., the encrypted digital data that has been received by the data transmit/receive unit 100. Meanwhile, in a secure area on the primary recording medium 102, encrypted accounting information, for instance, is recorded by the accounting unit 118 when the downloaded music data is recorded on the secondary recording medium 114.

[0041] Fig. 4 shows an example of the data structure of downloaded music data stored in the primary recording medium 102, i.e., music data that the information provider provides. Music data provided by the information provider mainly composed of attribute information 401 including the title, singer, and price of the music data and a music data unit 402 that is the music data itself.

[0042] The attribute information 402 includes ISRC (International Standard Recording Code) information 403, a title 404, a singer 405, a price 406, an information provider 407, and an encryption format 408. An explanation of the attribute information 401 will be given below.

[0043] The ISRC information 403 is specific information assigned to each piece of music data, and is composed of a country code (two ASCII (American Standard Cord for International Interchange) characters), an owner code (three ASCII characters), a recording year (two-digit numbers), and a serial number (five-digit numbers). The title 404 is character information showing the title of the music data and the singer 405 is character information showing the singer of the music data. The price 406 is information showing the data of the music data. Note that the price 406 shows the amount that is charged when the downloaded music data is recorded on the secondary recording medium 114 using the digital data recording apparatus in the present embodiment.

[0044] The information provider 407 is information showing the provider or the copyrighter of the music data, i.e., shows the recipient of the amount charged when the user records the music data using the digital data recording apparatus.

[0045] The encryption format 408 is information showing the encryption format in which the downloaded music data has been encrypted because the encryption format of music data depends on the information pro-

vider. For instance, when information providers A, B, and C provide music data, music data provided by the information provider A is encrypted in a format A, music data provided by the information provider B is encrypted in a format B, and music data provided by the information provider is encrypted in a format C. Note that the main object of the invention in the present embodiment is to convert data on the secondary recording medium 114 according to an encryption format that is easily decoded by a playback apparatus and to protect the copyright when information provided by information providers are encrypted in a variety of formats. As a result, a detailed explanation of the algorithm of encryption will not given here.

[0046] In the attribute information 401, the price 406 and the information provider 407 are encrypted as necessary since the tampering of the price 406 and the information provider 407 can lead to a loss to the information provider.

[0047] When receiving an instruction from the encryption system designation unit 109 to extract digital data, the data extraction unit 103 extracts the attribute information 401 from the primary recording medium 102 and informs the accounting unit 118 of the attribute information 401. Meanwhile, the data extraction unit 103 informs the judging unit 104 of information in the encryption format 408. Note that when the price 406 is encrypted in the attribute information 401, the data extraction unit 103 informs the accounting unit 118 of the price 406 after the decoding by the decryption unit group 105. Then, the data extraction unit 103 extracts the music data unit 402 from the primary recording medium 102, and outputs the extracted music data unit 402 to the judging unit 104. As has been described, the data extracted by the data extraction unit 103 has been encrypted in an encryption system specific to the information provider.

[0048] The judging unit 104 judges to which decryption unit the music data is to be output according to the information of the encryption format 408 that has been informed of by the data extraction unit 103.

[0049] The decryption unit group 105 includes "n" decryption units. A first decryption unit 106 decodes digital data that has been encrypted in the format A, a second decryption unit 107 decodes digital data that has been encrypted in the format B, and an "n"th decryption unit 108 decodes digital data that has been encrypted in the format N. Each of the first, second, and nth decryption units 106, 107, and 108 is composed of the decode module of a different information provider.

[0050] For instance, when the information of the encryption format 408 indicates the format B, the judging unit 104 outputs the digital data in the music data unit 402 in the music data to the second decryption unit 107. The second decryption unit 107 decodes the input digital data and outputs the decoded digital data to the encryption system designation unit 109.

[0051] When a decryption key is necessary to

decrypt encrypted data by one of the first, second, and nth decryption units 106, 107, and 108, the data transmit/receive unit 100 obtains a decryption key according to the encryption system of the data to decrypt the data. The first, second, and nth decryption units 106, 107, and 108 once decrypt data that has been encrypted in a different encryption system according to the information provider.

[0052] When having received the designation of the kind of encryption system from the designation reception unit 117, the encryption system designation unit 109 instructs the inherent information obtaining unit 116 to obtain inherent information according to the designation. When notified of the inherent information by the inherent information obtaining unit 116, the encryption system designation unit 109 instructs the data extraction unit 103 to extract music data. When notified that the inherent information according to the designation cannot be obtained by the inherent information obtaining unit 116, the encryption system designation unit 109 shows that the designated encryption system cannot be used to re-encrypt data on the display unit (not illustrated). Meanwhile, when not having received the designation of the kind of encryption system from the designation reception unit 117, the encryption system designation unit 109 instructs the inherent information obtaining unit 116 to obtain inherent information according to the attribute of the secondary recording medium 114. When receiving the notification concerning the obtainment of the inherent information from the inherent information obtaining unit 116, the encryption system designation unit 109 instructs the data extraction unit 103 to extract music data. When notified that the inherent information cannot be obtained, the encryption system designation unit 109 generates random numbers.

[0053] When having received the designation of the kind of encryption system from the designation reception unit 117, the encryption system designation unit 109 selects one encryption unit according to the designation. When receiving the input of decrypted digital data from one of the first, second, nth decryption units 106, 107, and 108, the encryption system designation unit 109 notifies the selected encryption unit of the decrypted digital data along with the inherent information that has been informed of by the inherent information obtaining unit 116.

[0054] When not having received the designation of the kind of encryption system from the designation reception unit 117, the encryption system designation unit 109 selects one encryption unit according to the kind of the inherent information that has been informed of by the inherent information obtaining unit 116. When receiving the input of decrypted digital data from one of the first, second, nth decryption units 106, 107, and 108, the encryption system designation unit 109 notifies the selected encryption unit of the digital data along with the inherent information. Meanwhile, when having received the notification that the inherent information

cannot be obtained from the inherent information obtaining unit 116, the encryption system designation unit 109 notifies one of the encryption units of the digital data along with generated random numbers.

[0055] The encryption unit group 110 includes "n" encryption units, a first, second, ..., "n"th encryption units 111, 112, ..., 113. Each of the encryption units 111, 112, ..., 113 re-encrypts informed digital data with a different encryption key. More specifically, the first encryption unit 111 re-encrypts data with an encryption key that is created according to the identification information inherent in the secondary recording medium 114. The second encryption unit 112 re-encrypts data with an encryption key that is created according to the identification information inherent in a playback apparatus for playing back the secondary recording medium 114 (not illustrated). The nth encryption unit 113 re-encrypts data with an encryption key that is created according to random numbers. Each of the data size of the encryption keys is set smaller than the data size of the encryption key of encrypted digital data that is recorded on the primary recording medium 102.

[0056] When the data size of the encryption key of re-encrypted digital data that is to be recorded on the secondary recording medium recording medium 114 is relatively small, the digital data is decrypted relatively easily. As a result, the structure necessary to decrypt the digital data of a playback apparatus for playing back the digital data is simple, leading to reduce the cost of the playback apparatus.

[0057] For instance, when having received no instruction from the designation reception unit 117 and having been informed of the identification information of the secondary recording medium 114 from the inherent information obtaining unit 116, the encryption system designation unit 109 informs the first encryption unit 111 of the identification information of the secondary recording medium 114. The first encryption unit 111 creates an encryption key according to the informed identification information, rewrites the encryption format 408 of the attribute information 401 of the music data that has been informed of by the encryption system designation unit 109, and re-encrypts the music data unit 402 using the created encryption key. The first encryption unit 111 informs the recording unit 115 of the re-encrypted digital data.

[0058] When having received the instruction to re-encrypt data using the inherent information of a playback apparatus for playing back the secondary recording medium 114 (not illustrated) from the designation reception unit 117, the encryption system designation unit 109 instructs the inherent information obtaining unit 116 to obtain the identification information inherent in the playback apparatus. When informed of the identification information inherent in the playback apparatus from the inherent information obtaining unit 116, the encryption system designation unit 109 informs the second encryption unit 112 of the informed identification

information and the decrypted digital data that has been informed of from the decryption unit group 105.

[0059] The second encryption unit 112 creates an encryption key according to the identification information that has been transferred from the encryption system designation unit 109, re-encrypts the digital data with the created encryption key, and informs the recording unit 115 of the re-encrypted digital data. As in the case of not having received the instruction from the designation reception unit 117, the content of the encryption format 408 in the attribute information 401 is rewritten.

[0060] The secondary recording medium 114 is composed of a DVD-RAM disc (shown in Fig. 2), an MD, and a small-scale semiconductor memory that is removable or nonremovable according to the model of a playback apparatus (not illustrated) and the like. Music data that has been re-encrypted by the encryption unit group 110 is recorded on the secondary recording medium 114 by the recording unit 115. For instance, when digital data has been recorded on the DVD-RAM disc 203, the DVD-RAM disc 203 is inserted into the DVD-Audio player 204 to play music as shown in Fig. 2.

[0061] The recording unit 115 is realized by, for instance, the DVD-RAM drive 202 shown in Fig. 2. The recording unit 115 records digital data that has been transferred from the encryption unit group 110 on the secondary recording medium 114. When completing recording, the recording unit 115 informs the accounting unit 118 of the completion.

[0062] When having instructed to obtain the identification information inherent in the secondary recording medium 114 by the encryption system designation unit 109, the inherent information obtaining unit 116 reads the information written in the BCA (Burst Cutting Area) and informs the encryption system designation unit 109 of the read information when the secondary recording medium 114 is a DVD-RAM, for instance. Note that each secondary recording medium 114 has a different piece of inherent identification information that has been recorded at the time of manufacturing, so that the identification information cannot be read or rewritten by ordinary user operation.

[0063] An encryption key is created according to the identification information, and digital data re-encrypted with the encryption key is recorded on a DVD-RAM disc. As a result, even if a user with a malicious intent makes a copy of the content of the DVD-RAM disc on another recording medium using a tool for bit copy and tries to play back the copied data on other recording medium, the copied data cannot be normally decrypted since the information for decryption key of the other recording medium is different from that of the DVD-RAM disc. In this way, the copyright of the music data is fully protected.

[0064] Meanwhile, when having been instructed to obtain the identification information inherent in the playback apparatus (not illustrated) in which the secondary

recording medium 114 is put by the encryption system designation unit 109, the inherent information obtaining unit 116 reads the identification information of the playback apparatus and informs the encryption system designation unit 109 of the read identification information. Each playback apparatus also has a different piece of inherent identification information that has been assigned at the time of manufacturing, so that the identification information cannot be read or rewritten by an ordinary user operation. As a result, when data is re-encrypted according to identification information, the re-encrypted data can be played back only by a peculiar playback apparatus.

[0065] Note that when the inherent information obtaining unit 116 cannot obtain the inherent identification information that has been designated by the encryption system designation unit 109, i.e., when no identification information is assigned to the secondary recording medium 114 and the playback apparatus, the inherent information obtaining unit 116 informs the encryption system designation unit 109 that the designated inherent identification information cannot be obtained.

[0066] When receiving the instruction to obtain inherent identification information without the instruction of the kind of the inherent identification information, the inherent information obtaining unit 116 judges whether the secondary recording medium 114 is a recording medium removable from the playback apparatus such as a DVD-RAM disc or a recording medium that is built in the playback apparatus such as a small-scale semi-conductive memory. When the secondary recording medium 114 is a removable one, the inherent information obtaining unit 116 reads the inherent identification information of the secondary recording medium 114, and informs the encryption system designation unit 109 of the read inherent identification information. Meanwhile, when the secondary recording medium 114 is a nonremovable one, the inherent information obtaining unit 116 reads the inherent identification information of the playback apparatus, and informs the encryption system designation unit 109 of the read inherent identification information. When no identification information can be obtained, the inherent information obtaining unit 116 informs the encryption system designation unit 109 that no identification information can be obtained.

[0067] The designation reception unit 117 is realized by the keyboard and the mouse of the PC. The designation reception unit 117 receives the instruction of the kind of encryption system from the user, and informs the encryption system designation unit 109 of the encryption system kind.

[0068] While the homepage information in Fig. 3 shows only one type of price, the homepage information in Fig. 5 shows two types of price, i.e., a price (1) 501 and a price (2) 502.

[0069] While the price (1) 501 shows the price when digital data is re-encrypted at the time of record-

ing according to the identification information inherent in the secondary recording medium 114, the price (2) 502 shows the price when digital data is re-encrypted at the time of recording according to the identification information inherent in the playback apparatus for playing back the secondary recording medium 114. Note that each of the prices (1) 501 and (2) 502 is freely set by the information provider.

[0070] The user instructs the encryption of digital data in a desired encryption format in reference to the music and price information shown in Fig. 5 according to the usage pattern of the secondary recording medium 114 using the designation reception unit 117. For instance, when digital data is to be played back in a specific playback apparatus, i.e., when the secondary recording medium 114 is not played back in other playback apparatuses, the user instructs to re-encrypt the digital data according to the identification information inherent in the specific playback apparatus. As shown by the price (2) in Fig. 5, prices are generally cheap when data is re-encrypted according to the identification information of playback apparatus. This is because the degree of freedom is low compared with the encryption according to the identification information inherent in the secondary recording medium 114 since re-encrypted data is not played back in other playback apparatuses. When digital data is to be played back with any playback apparatus, the user instructs to re-encrypt the digital data according to the identification information inherent in the secondary recording medium 114.

[0071] Note that although the designation reception unit 117 is integral with the reception unit 101, the designation reception unit 117 and the reception unit 101 are described as separate elements for convenience in explanation.

[0072] The accounting unit 118 receives the notification of the attribute information 401 of music data from the data extraction unit 103 and stores the received attribute information 401. When notified that re-encrypted digital data is recorded on the secondary recording medium 114 by the recording unit 115, the accounting unit 118 refers to the price 406 in the attribute information 401 to determine the amount of charge and writes the determined amount of charge along with the attribute information 401 in a secure area on the primary recording medium 102 as the accounting information.

[0073] Note that when the price 406 includes the prices (1) 501 and (2) 502 as shown in Fig. 5, the amount of charge is determined according to one of the first to nth encryption units 111 to 113 that has been transferred to the accounting unit 118 as the used encryption unit from the encryption system designation unit 109.

[0074] Here, an explanation of the operations in the present embodiment will be given with reference to the flowcharts in Figs. 6 and 7.

[0075] The reception unit 101 receives home page

requirement from the user, the data transmit/receive unit 100 accesses to a homepage provided by an information provider of music data, and the data extraction unit 103 displays a homepage (refer to Figs. 3 and 5) on the display unit (not illustrated) (step s602).

[0076] The data extraction unit 103 awaits instruction to purchase music data designated by the user from the reception unit 101 and instructs the data transmit/receive unit 100 to receive the designated music data (step s604). When receiving the music data, the data transmit/receive unit 100 downloads the received music data on the primary recording medium 102 (s606).

[0077] Watching the homepage display, the user inputs the kind of encryption system according to the usage pattern of the secondary recording medium 114 using the designation reception unit 117.

[0078] The encryption system designation unit 109 judges whether the designation reception unit 117 has informed the encryption system designation unit 109 of the designation of the kind of encryption system (step s608). When having been informed of the designation of the kind of encryption system, the encryption system designation unit 109 instructs the inherent information obtaining unit 116 to obtain the inherent information that is to be used for the encryption system of the designated kind (step s610). The encryption system designation unit 109 judges whether the inherent information obtaining unit 116 has informed that the inherent information cannot be obtained (step s612). When informed that the inherent information cannot be obtained, the encryption system designation unit 109 has the display unit (not illustrated) display that the music data cannot be re-encrypted according to the encryption system of the designated kind (step s614) to complete the processing. Meanwhile, when informed of the inherent information for the designated kind of encryption system, the encryption system designation unit 109 instructs the data extraction unit 103 to extract the digital data.

[0079] The data extraction unit extracts the music data recorded on the primary recording medium 102 (step s616).

[0080] At step s608, when judging that the designation reception unit 117 has not informed the encryption system designation unit 109 of the designation of the kind of encryption system, the encryption system designation unit 109 instructs the inherent information obtaining unit 116 to obtain inherent information without designating the kind of the inherent information (step s618).

[0081] The inherent information obtaining unit 116 judges the attribute of the secondary recording medium 114, i.e., judges whether the secondary recording medium 114 in the playback apparatus (not illustrated) is a removable one. When the secondary recording medium 114 is a removable one, the inherent information obtaining unit 116 obtains the identification informa-

tion of the secondary recording medium 114, and when the secondary recording medium 114 is a nonremovable one, the inherent information obtaining unit 116 obtains the identification information of the playback apparatus (step s620).

[0082] When informed of the inherent (identification) information by the inherent information obtaining unit 116, or when informed that inherent information has not been obtained (step s622), the encryption system designation unit 109 instructs the data extraction unit 103 to extract the digital data. The processing advances to step s616.

[0083] Then, the judging unit 104 refers to the encryption format 408 in the attribute information 401 of the music data that has been extracted by the data extraction unit 103 and judges which one of the first to nth decryption units 106 to 108 in the decryption unit group 105 decrypts the music data (step s702).

[0084] One of the first to nth decryption units 106 to 108 that has been judged by the judging unit 104 decrypts the digital data that has been input via the judging unit 104 and outputs the decrypted digital data to the encryption system designation unit 109 (step s704).

[0085] The encryption system designation unit 109 selects one of the first to nth encryption units 111 to 113 in the encryption unit group 110 according to the inherent information that has been transferred from the inherent information obtaining unit 116 (including the information that inherent information cannot be obtained), and informs the selected encryption unit of the inherent information (generated random numbers in the case of the information that inherent information cannot be obtained) and the decrypted digital data (step s706).

[0086] The informed encryption unit creates an encryption key according to the inherent (identification) information (according to the random numbers in the case of the information of the random numbers) and re-encrypts the digital data using the created encryption key. At this time, the content of the encryption format 408 is rewritten in the attribute information 401 (step s708).

[0087] The recording unit 115 records the digital data on the secondary recording medium 114 that has been transferred from one of the first to nth encryption units 111 to 113 (step s710). When completing the recording, the recording unit 115 informs the accounting unit 118 of the recording completion.

[0088] When receiving the information from the recording unit 115, the accounting unit 118 determines the amount of charge according to the price 406 and the like that has been transferred from the data extraction unit 103 and records the amount of charge on the primary recording medium 102 (step s712) to complete the processing.

[0089] In the present embodiment, the decryption unit group 105 are composed of the decryption modules

(the first to nth decryption units 106 to 108) for different information providers. The decryption unit group may include different decryption units according to the quality of music data, for instances, for digital data in 24 bits of LPCM (Liner Pulse Code Modulation), MP3 (Moving Picture Experts Group 1 Audio Layer 3) and the like. More specifically, while high quality 24 bits of LPCM may be set as encrypted digital data that is difficult to decrypt, normal MP3 may be set as encrypted digital data that is not so difficult to decrypt, and the first decryption unit 106 may decrypt digital data in 24 bits of LPCM and the second decryption unit 107 may decrypt digital data in MP3.

[0090] In the present embodiment, the encryption unit group 110 includes the first to nth encryption units 111 to 113 for different kinds of inherent information. The encryption units may correspond to the quality of music data. More specifically, digital data that has been decrypted by the first decryption unit 106 may be re-encrypted by the first encryption unit 111, digital data that has been decrypted by the second decryption unit 107 may be re-encrypted by the second encryption unit 112, and digital data that has been decrypted by the nth decryption unit 108 may be re-encrypted by the nth encryption unit 113. In this case, the data size of the encryption key used for encryption in the first encryption unit 111 is larger than that of the encryption key used in the second encryption unit 112, and that of the encryption key used in the second encryption unit 112 is larger than that of the encryption key used in the nth encryption unit 113. The accounting unit determines the accounting amount of digital data according to the decryption unit that has decrypted the digital data and the encryption unit that has re-encrypted the digital data. As a result, the higher the quality of digital data, the more surely the copyright is protected. In this case, information provider may set higher price for music data with higher quality.

[0091] The digital data recording apparatus according to the present embodiment has the structure shown in Fig. 1. It is possible to record a program on a computer-readable recording medium such as a floppy disk that has a computer realize the functions of the elements of the digital data recording apparatus, and to protect copyrights by applying the computer readable recording medium to a digital data recording apparatus that has no function of protecting copyrights.

[0092] In the present embodiment, digital data is downloaded from the host computer when the user requires the purchase of the digital data. It is possible to temporarily record music data or only the attribute information on the primary recording medium in the PC of the user regardless of the purchase, and to purchase digital data that has been recorded on the primary recording medium 102.

[0093] While the attribute information 401 and the music data unit 402 are separately described in the present embodiment, the attribute information 401 may

be embed in the digital data in the music data 402 using Water Mark (electronic watermark) technology.

[0094] In the present embodiment, the data input and output between the decryption unit group 105 and the encryption unit group 110 via the encryption system designation unit 109 has not been referred to in particular. It is possible to prevent the leakage of decrypted data for security by transmitting data after authentication or by realizing the decryption unit group 105, the encryption system designation unit 109, and the encryption unit group 110 with one chip.

[0095] In addition, while accounting information is recorded in a secure area on the primary recording medium 102 in the present embodiment, accounting information may be recorded on another recording medium such as an IC card.

[0096] No explanation of the timing of accounting has been given in the present embodiment. It is possible to suppose that the modem is connected to the host computer when digital data is recorded on the secondary recording medium 114, to suppose that the modem is automatically connected to the host computer when the amount of charge reaches to a set amount, or to suppose that the modem is connected to the host computer when a set period of time has elapsed since the recording of accounting information.

[0097] In addition, while only audio information is provided by the information provider in the present embodiment, video information, audio information, character information, the combination of video information, audio information, and character information, and the like may be provided.

(The Second Embodiment)

[0098] Fig. 8 shows the structure of a digital data recording apparatus according to the second embodiment of the present invention. The digital data recording apparatus is generally realized by a personal computer. The digital data recording apparatus includes a data transmit/receive unit 2101, a primary recording medium 2102, a data extraction unit 2103, an encryption system judging unit 2104, a first decryption unit 2105, a second decryption unit 2106, a third decryption unit 2107, an encryption unit 2108, a recording unit 2109, a secondary recording medium 2110, an input unit 2111, a display unit 2112, and a recording medium inherent information obtaining unit 2113. While a decryption unit group 2115 is composed of the first, second, third decryption units 2105, 2106, and 2107, the number of decryption units is not limited to three. The decryption unit group 2115 is composed of a plurality of decryption units.

[0099] Note that data to be recorded are music data that are distributed through the Internet in the present embodiment. The music data are supposed to be encrypted in different encryption systems according to the providers.

[0100] An information provider provides music data and information including music titles, prices, copy control information, and the like (referred to "attribute information" in this specification) that are necessary at the time of purchase and may arouse the interest of users together or separately. In the present embodiment, attribute information and music data are supposed to be separately provided.

[0101] The data transmit/receive unit 2101 is a communication unit realized by a modem and is connected to the host computer (not illustrated) of the information provider through a telephone line. The attribute information that the data transmit/receive unit 2101 has obtained is recorded on the primary recording medium 2102, and the entire attribute information or part of it is displayed on the display unit 2112. Fig. 9 is an example of information displayed on the display unit 2112. Information such as titles 2201, title codes 2202, singers 2203, data sources 2204 are displayed. Here, a title 2201 and a singer 2203 show the title and singer of one piece of music data. A title code 2202 is an identifier for distinguishing one piece of music data from another piece of music data. To a title code 2202, a piece of ISRC (International Standard Recording Code) information is added to, for instance. According to the information, the user selects a piece of desired music and transfers the purchase requirement with the input unit 2111. A data source 2204 is a URL (Uniform Resource Locator) for specifying the location of a piece of music data. When ISRC information is added to a title code 2202, the data source can be identified by the title code 2202.

[0102] The input unit 2111 is realized by a mouse, a keyboard, and the like. The input unit 2111 receives an instruction to purchase music, i.e., a recording instruction, and informs the data transmit/receive unit 2101 of the instruction. The user clicks the title and the like of the selected music with the mouse according to information displayed on the display unit 2112 to instruct the recording of the music data.

[0103] When receiving the instruction to record the music data, the data transmit/receive unit 2101 downloads the desired music data from the host computer of the provider through the telephone line. At this time, the location of the music data is specified according to the URL in the attribute information. The music data downloaded is once recorded on the primary recording medium 2102.

[0104] The primary recording medium 2102 is generally a hard disk in the PC, and records the desired music data without decrypting. As a result, the digital data recording apparatus is not necessarily connected to the host computer of the provider during the following operations.

[0105] The data extraction unit 2103 extracts the music data to be recorded from the primary recording medium 2102. At this time, the user selects the music data to be recorded on the secondary recording

medium 2110 with the input unit 2111 according to the information displayed on the display unit 2112 that is almost equivalent to the information shown in Fig. 9. The data extracted by the data extraction unit 2103 has been encrypted in an encryption system according to the information provider, so that the encryption system judging unit 2104 judges an appropriate system to decrypt the data. For example, information for identifying the encryption system of digital data is added to the header, or the attribute information indicates the encryption system, and the encryption system judging unit 2104 judges the encryption data according to the information.

[0106] The first, second, and third decryption units, 2105, 2106, and 2107 show that digital data are decrypted in different systems according to the information providers. The number of decryption units is not limited to three. The encryption system judging unit 2104 selects one appropriate decryption unit, and the selected decryption unit decrypts encrypted data. More specifically, the encryption system judging unit 2104 obtains or creates a decryption key corresponding to the obtained encryption system of the data, and the selected decryption unit decrypts the data with the decryption key. As a result, data that have been encrypted in different encryption systems are once decrypted.

[0107] The encryption unit 2108 re-encrypts the decrypted data. In the present embodiment, information inherent in the recording medium is supposed to be used as the encryption key information at the time of encryption. Note that a method of encryption according to information inherent in a recording medium is described in Japanese Laid-Open Patent Application No. 05-257816, so that a detailed explanation will not be given here.

The recording medium inherent information obtaining unit 2113 extracts the inherent information from the secondary recording medium 2110 according to an instruction from the encryption unit 2108, and transfers the extracted inherent information to the encryption unit 2108.

[0108] The encryption unit 2108 re-encrypts data using the inherent information that has been obtained by the recording medium inherent information obtaining unit 2113 as the encryption key.

[0109] Here, an explanation of the information inherent to the secondary recording medium 2110 will be given.

[0110] Each secondary recording medium 2110 has a different inherent identification information. When a secondary recording medium 2110 is a DVD-RAM, the inherent identification information is the information written in the BCA (Burst Cutting Area). Each disc has a different information in the BCA, and the information is recorded at the time of manufacturing and is not rewriteable. As a result, even if a user with a malicious intent makes a copy of the content of the disc on another

recording medium using a tool for bit copy, the copied data cannot be decrypted since the information for decryption key of the other recording medium is different from that of the disc. In this way, the copyright of the data is surely protected.

[0111] The recording unit 2109 records the re-encrypted data on the secondary recording medium 2110.

[0112] An explanation of the operations by the digital data recording apparatus the structure of which has been described will be given with reference to the flow-chart in Fig. 10.

[0113] The data transmit/receive unit 2101 downloads the attribute information (step s2301), and awaits for an instruction to record digital data from the user (step s2302). The data transmit/receive unit 2101 downloads designated digital data and records the digital data on the primary recording medium 2102 (step s2303). The encryption system of the downloaded data is judged, and an appropriate one of the first, second, and third decryption units 2105, 2106, and 2107 is instructed to decrypt the data (step s2304). One of the first, second, and third decryption units 2105, 2106, and 2107 decrypts the data (step s2305). When the decrypted data is input, the encryption unit 2108 obtains the inherent information of the secondary recording medium 2110 from the recording medium inherent information obtaining unit 2113 (step s2306). An encryption key is created using the obtained inherent information as part of the encryption key, and the encryption unit 2108 re-encrypts the data (step s2307). The recording unit 2109 records the re-encrypted data on the secondary recording medium 2110 (step s2308), where the processing is completed.

[0114] An explanation has been given of the digital data recording apparatus according to the second embodiment of the present invention.

[0115] An explanation of a digital data recording apparatus according to the third embodiment of the present invention will be given below.

(The Third Embodiment)

[0116] Fig. 11 shows the structure of the digital data recording apparatus according to the third embodiment of the present invention. The digital data recording apparatus is generally realized by a PC. The digital data recording apparatus includes a data transmit/receive unit 2101, a primary recording medium 2102, a data extraction unit 2103, an encryption system judging unit 2104, a decryption unit group 2115, an attribute information obtaining unit 2401, a copy control information detection judging unit 2402, a copy control information conversion unit 2403, an accounting information calculation unit 2404, an encryption unit 2108, a secondary recording medium 2110, an input unit 2111, a display unit 2112, and a recording medium inherent information obtaining unit 2113.

[0117] Note that the elements of the digital data recording apparatus that are the same in the second and third embodiments have the same reference numbers and explanations of the elements are not given below.

[0118] Fig. 12 shows the attribute information of data in the present embodiment. The attribute information in Fig. 12 includes copy control information 2501 and accounting information 2502 in addition to the attribute information shown in Fig. 9. The copy control information 2501 shows the number of times data can be recopied or copied. For instance, in terms of the number of times data can be recopied, a value corresponding to "no limit", "copying only (no recopying)", "no copying" and the like is shown. On the other hand, the number of times data can be copied is an integer larger than "0". More specifically, "no recopying" means that digital data that has been recorded on a secondary recording medium 2110 cannot be recopied. "No limit" means that the data can be copied any number of times. The copying times, such as, "two copies" means that data can be copied on two secondary recording media 2110.

[0119] The attribute information obtaining unit 2401 obtains attribute information corresponding to data to be reproduced from the primary recording medium 2102. In the present embodiment, the copy control information and the accounting information 2502 are extracted. Note that since attribute information includes copyright protection information and the accounting information 2502, it is desirable to record attribute information in a secure area on the primary recording medium 2102 so that attribute information could not be accessed by an ordinary user operation.

[0120] The copy control information detection judging unit 2402 extracts the copy control information from the attribute information to obtain the information indicating whether copying or recopying is allowed and the number of times data can be copied or recopied.

[0121] When copying or recopying is allowed, the copy control information conversion unit 2403 rewrites the copy control information as necessary. For instance, when recopying is prohibited, the copy control information conversion unit 2403 changes the value of the copy control information 2501 so that recopying would be prohibited. When the number of times data is copied is limited, the copy control information conversion unit 2403 changes the value so that the value would be the number that is less than the copying number allowed by "1".

[0122] When the allowed copying number is set, what is important is the number of times the data on the primary recording medium 2102 is recorded on the secondary recording medium 2110. The rewriting of the copy control information is to rewrite data recorded on the primary recording medium 2102. As a result, the allowed copying number that has been recorded on the primary recording medium 2102 is decreased by "1",

and the allowed copying number that is to be recorded on the secondary recording medium is "0".

[0123] The accounting information calculation unit 2404 obtains the accounting information of the desired music data from the attribute information that has been obtained by the attribute information obtaining unit 2401, calculates the amount of charge according to the accounting information, and records the calculated amount of charge in a secure area on the primary recording medium 2102.

[0124] An explanation of the operations by the digital data recording apparatus, the structure of which has been described, will be given with reference to the flowcharts in Figs. 13 and 14.

[0125] First, the data transmit/receive unit 2101 downloads the attribute information (step s2601), awaits a recording instruction of digital data from the user (step s2602), downloads the designated digital data, and records the downloaded digital data on the primary recording medium 2102 (step s2603). Then, the data transmit/receive unit 2101 obtains the attribute information of the data to be recorded from the attribute information obtaining unit 2401 (step s2604). The copy control information detection judging unit 2402 judges the copy control information 2501 in the attribute information and judges whether copying is allowed (step s2605). When copying is allowed, the allowed number of times of recopying or copying is obtained, and the obtained number of times is rewritten by the copy control information conversion unit 2403 as necessary (step s2606). When copying is not allowed, the processing will be discontinued (step s2607). Then, the encryption system is judged, and an appropriate decryption unit in the decryption unit group 2115 is instructed to decrypt the digital data (step s2608). One of the first, second, and third decryption units decrypts the digital data (step s2609). After the decryption, the amount of charge is calculated according to the accounting information that has been obtained by the attribute information obtaining unit 2401 (step s2610).

[0126] Receiving the decrypted data, the encryption unit 2108 obtains the inherent information of the secondary recording medium 2110 from the recording medium inherent information obtaining unit 2113 (step s2611). An encryption key is created including the obtained inherent information as part, and encryption unit 2108 re-encrypts the data (step s2612). The recording unit 2109 records the re-encrypted data on the secondary recording medium 2110 (step s2613), and the processing is completed.

[0127] Up to this point, an explanation of the third embodiment of the present invention has been given.

(The Fourth Embodiment)

[0128] An explanation of a digital data recording apparatus according to the fourth embodiment of the present invention will be given. The digital data record-

ing apparatus is different from the digital data recording apparatus in the second embodiment in encryption key information and in including an inherent information obtaining/transfer unit 2803, a recording unit 2109, and a secondary recording medium 2110 in a second digital data recording apparatus 2801. Fig. 15 shows the structure of the digital data recording apparatus according to the fourth embodiment of the present invention. The digital data recording apparatus is composed of first and second digital data recording apparatuses 2800 and 2801.

[0129] The first digital data recording apparatus 2800 includes a data transmit/receive unit 2101, a primary recording medium 2102, a data extraction unit 2103, an encryption system judging unit 2104, a decryption unit group 2115, an encryption unit 2108, an input unit 2111, a display unit 2112, and an inherent information obtaining unit 2802.

[0130] The second digital data recording apparatus 2801 includes the inherent information obtaining/transfer unit 2803, the recording unit 2109, and the secondary recording medium 2110.

[0131] Note that the elements of the digital data recording apparatus in the fourth embodiment that are the same in the second embodiment have the same reference numbers and explanations of the elements are not given below.

[0132] When the data that has been decrypted in the decryption unit group 2115 is input into the encryption unit 2108, the inherent information obtaining unit 2802 requires the inherent information obtaining/transfer unit 2803 in the second digital data recording apparatus 2801 to transfer inherent information. The inherent information obtaining/transfer unit 2803 obtains the identification information inherent in the secondary recording medium 2110 in the second digital data recording apparatus 2801 or the identification information inherent in the second digital data recording apparatus 2801, and transfer the obtained identification information to the inherent information obtaining unit 2802.

[0133] The encryption unit 2108 creates an encryption key using the identification information inherent in the secondary recording medium 2110 in the second digital data recording apparatus, the identification information inherent in the second digital data recording apparatus 2801, or the combination of these identification information, and re-encrypts the decrypted data, and outputs the re-encrypted data to the second digital data recording apparatus 2801. The recording unit 2109 in the second digital data recording apparatus 2801 records the re-encrypted data on the secondary recording medium 2110.

[0134] Note that inherent information that is obtained and transferred by the inherent information obtaining/transfer unit 2803 is the identification information inherent in the second digital data recording apparatus 2801 when the secondary recording medium 2110

is fixed in the second digital data recording apparatus 2801, and is the identification information inherent in the secondary recording medium 2110 or the combination of the identification information inherent in the second digital data recording apparatus 2801 and the identification information inherent in the secondary recording medium 2110 when the secondary recording medium 2110 is removable from the second digital data recording apparatus 2801. As a result, more flexible encryption systems can be available.

[0135] Up to this point, an explanation of the fourth embodiment of the present invention has been given.

(The Fifth Embodiment)

[0136] Here, an explanation of a digital data recording apparatus according to the fifth embodiment of the present invention will be given. The digital data recording apparatus is almost the same as those in the second, third, and fourth embodiment. The explanation of the digital data recording apparatus will be given with reference to the block diagram in Fig. 15 used in the fourth embodiment. The digital data recording apparatus in the fifth embodiment is different from that in the fourth embodiment in adopting an encryption system corresponding to the secondary recording medium 2110 at the time of recording. More specifically, since the minimum unit of data, or the unit of data amount at the time of writing encrypted data is different for a DVD-RAM and a semiconductor memory, the inherent information obtaining unit 2802 obtains information of the medium from the inherent information obtaining/transfer unit 2803 to re-encrypt data in an optimal unit of data. As a result, a plurality of encryption units 2108 are included and inherent information and medium information are transferred to an appropriate encryption unit. By doing so, not only a DVD-RAM but also a semiconductor memory, an IC card, and a hard disk can be used as the secondary recording medium 2110.

[0137] Up to this point, an explanation of the fifth embodiment has been given.

[0138] Note that the second to fifth embodiments have been explained as examples of system by which optimal effects can be expected under the present situation. The embodiments can be changed within the range of the basic principles of the present invention. Examples of changed embodiments will be given below.

[0139] In the second to fifth embodiments, digital data is downloaded from the host computer when the user requests to purchase the digital data. It is possible to record digital data on the primary recording medium 2102 in the user's PC regardless of the purchase and to request to purchase digital data that has been recorded on the primary recording medium 2102.

[0140] In the second to fifth embodiments, copy control information is indicated in attribute information. It is possible to embed copy control information into digital data using Water Mark technology.

[0141] While it has been explained that accounting information is recorded in a secure area on the primary recording medium 2102, it is possible to provide another recording medium such as an IC card than the primary recording medium 2102 to record accounting information.

[0142] While the information provided by the information provider is audio information in the second to fifth embodiments, the information is not limited to audio information. The information can be video information, audio information, character information, or the combination of video, audio, and character information.

(The Sixth Embodiment)

[0143] Fig. 16 shows the structure of a digital data recording apparatus according to the sixth embodiment of the present invention.

[0144] The digital data recording apparatus includes a communication unit 3101, a recording medium 3102, a received data record/judging unit 3103, a display unit 3104, an input operation unit 3105, a recording medium inherent information obtaining unit 3106, an encryption unit 3107, a recording unit 3108, an accounting information recording unit 3109, an accounting information recording medium 3110, and an accounting unit 3111. The digital data recording apparatus is realized by a PC.

[0145] The communication unit 3101 is realized by a modem, and is connected to the host computer (not illustrated) of a data provider and an accounting center (not illustrated) via a telephone line. When receiving digital data and the attribute information from the host computer, the communication unit 3101 informs the received data record/judging unit 3103 of the reception.

[0146] When receiving an inquiry of charge from the accounting center, the communication unit 3101 informs the accounting unit 3111 of the inquiry. When informed of accounting information by the accounting unit 3111, the communication unit 3101 informs the accounting center of accounting information via the telephone line.

[0147] Note that digital data provided by the data provider is supposed to be music data in the present embodiment. Music data to be provided is supposed to be encrypted digital data, and an information identifier is supposed to be added to a piece of digital data. The information identifier of a piece of music is supposed to be the title code for distinguishing the music from another piece of music.

[0148] Attribute information is also supposed to be added to a piece of digital data. Attribute information includes information indicating the charge and the provider of digital data.

[0149] Fig. 17 is an example of attribute information. Attribute information 3201 includes titles 3202, performers (singers) 3203, title codes 3204, recording charges 3205, charges per reproduction 3206, maxi-

num numbers of reproducing 3207, encryption conditions 3208, and copy permission 3209.

[0150] The titles 3202 and the performers 3203 are displayed on the display unit 3104. The user indicates to copy (replicate) digital data according to the titles 3202 and the performers 3203. A title code is unique to a piece of music for distinguishing the music from another piece of music. For instance, an ISRC is used as a title code 3204. Note that the ISRC is composed of a country code (two ASCII characters), an owner code (three ASCII characters), a recording year (two-digit numbers), and a serial number (five-digit numbers).

[0151] A recording charge 3205, a charge per reproduction 3206, a maximum number of reproducing 3207, and the like are included in accounting standard data, and are information for calculating the charges of a piece of music data.

[0152] A recording charge 3205 indicates a charge when digital data that has been received by the communication unit 3101 is recorded on the recording medium 3102. A charge per reproduction 3206 indicates the charge for reproducing digital data once that has been recorded on the recording medium 3102. A maximum number of reproducing 3207 indicates the maximum number of times that digital data that has been recorded on the recording medium 3102 can be reproduced. For instance, when a maximum number of reproducing 3207 is "100", the digital data can be reproduced up to 100 times. Note that it is possible to set a maximum number of reproducing 3207 so that no additional charge is required after the number of reproducing reaches a certain number of times.

[0153] An encryption condition 3208 is a flag showing whether digital data that has been received by the communication unit 3101 is an encrypted data.

[0154] Copy permission 3209 is a flag recorded by the user and shows whether it is permitted to record music data that has been received by the recording medium 3102. For instance, "only once" indicates that the music data is permitted to be recorded only once, and "permitted" indicates that the music data is permitted to be recorded any number of times.

[0155] Note that the main object of the present invention is to protect the copyright of received music data when the music data is recorded (replicated) on the recording medium 3102, so that an explanation of a case where it is only permitted to listen to music data will be given briefly. In this case, the copy permission 3209 is "not permitted". While neither decryption unit nor input unit is included in the structure shown in Fig. 16, digital data that has been received by the communication unit 3101 is decrypted by a decryption unit to input music from an input unit. At this time, the accounting standard data includes a listening charge.

[0156] The recording medium 3102 is composed of a rewriteable storage element such as a DVD-RAM and is removable from the digital data recording apparatus.

[0157] In a non-rewriteable secure area on the

recording medium 3102, inherent information of the recording medium 3102 is recorded in advance.

[0158] On the recording medium 3102, the digital data that has been re-encrypted by the encryption unit 3107 is recorded by the recording unit 3108.

[0159] In addition, the management information and attribute information of the recorded digital data are recorded on the recording medium 3102 by the recording unit 3108.

[0160] When informed of digital data and the attribute information 3201 from the communication unit 3101, the received data record/judging unit 3103 stores the attribute information 3201, has the display unit 3104 display the title 3202, the player 3203, the recording charge 3205, the charge per reproduction 3206 and the like, and informs the encryption unit 3107 of the digital data.

[0161] When receiving an instruction to copy (replicate) music, the received data record/judging unit 3103 judges whether the digital data corresponding to the title code 3204 of the designated music can be copied on referring to the copy permission 3209. When the digital data can be copied, the received data record/judging unit 3103 instructs the recording medium inherent information obtaining unit 3106 to obtain the inherent information of the recording medium 3102, and informs the encryption unit 3107 of the title code 3204 and the encryption condition 3208.

[0162] When it is not permitted to copy the digital data, the received data record/judging unit 3103 has the display unit 3104 display the judgement result.

[0163] When notified that the digital data has been copied by the recording unit 3108, the received data record/judging unit 3103 rewrites the copy permission 3209 in the stored attribute information 3201. More specifically, when the copy permission 3209 is "only once", the "only once" is changed to "not permitted". When the number of times of copying is greater than one, the number is decreased by one. Note that the storage area for storing the attribute information 3201 is in the EEPROM (Electrically Erasable and Programmable ROM), so that the storage content is not erased when the power of the digital data recording medium is turned off the storage content is not erased.

[0164] For instance, when informed of the completion of copying by the recording unit 3108 after informing the encryption unit 3107 of the title code 3204 "song01", the received at a record/judging unit 3103 changes the copy permission 3209 corresponding to the title code "song01" from "only once" to "not permitted". As a result, the violation of the data provider copyright can be protected.

[0165] The display unit 3104 is composed of a liquid crystal display or a CRT (Cathode-Ray-Tube). The display unit 3104 displays the title of music data (digital data) or indicates that the digital data cannot be copied under the control of the received data record/judging unit 3103.

[0166] The input operation unit 3105 is composed of a mouse and the like. The input operation unit 3105 receives the user's instruction to copy digital data and informs the received data record/judging unit 3103 of the instruction. When downloading a piece of music on referring to titles and players displayed by the display unit 3104, the user clicks the tile and the like with the mouse and instructs the copying of the music.

[0167] When receiving an instruction to obtain the inherent information from the received data record/judging unit 3103, the recording medium inherent information obtaining unit 3106 reads the inherent information that has been recorded in a secure area on the recording medium 3102 and informs the encryption unit 3107 of the read inherent information.

[0168] The encryption unit 3107 creates an encryption key according to the inherent information that has been received from the recording medium inherent information obtaining unit 3106. The encryption unit 3107 re-encrypts the digital data that has been received from the received data record/judging unit 3103 using the created encryption key and informs the recording unit 3108 of the re-encrypted digital data.

[0169] Note that when informed that the digital data that has been received from the received data record/judging unit 3103 has been encrypted, the encryption unit 3107 has the digital data be decrypted or use the digital data without a decryption.

[0170] More specifically, when informed of digital data "data A", which is to be recorded on the recording medium 3102, by the received data record/judging unit 3103, the encryption unit 3107 creates an encryption key "KM" according to the inherent information of the recording medium 3102 and re-encrypts the digital data "data A" to create encrypted digital data "E (KM, dataA)". When the digital data "dataA" is to be recorded on another recording medium and an encryption key "K'M" is created according to the inherent information of the other recording medium, the encrypted digital data "E" is encrypted digital data "E(K'M, dataA)".

[0171] The technology of digital data encryption is described in Japanese Laid-Open Patent Application No. 05-257816.

[0172] The recording unit 3108 records the encrypted digital data on the recording medium 3102 that has been received from the encryption unit 3107. At this time, the recording unit 3108 creates the management information of the recorded digital data on the recording medium 3102.

[0173] Fig. 18 shows an example of management information. Management information 3301 includes title codes 3204, which are the identifiers of recorded digital data, recording start addresses 3302, and recording end addresses 3303 of the recorded digital data. In the management information 3301, each of the title codes 3204 correspond to different recording start addresses 3302, and recording end addresses 3303.

[0174] When digital data recorded on the recording

medium 3102 is reproduced, the management information 3301 is referred to.

[0175] When finishing recording the encrypted digital data and the management information on the recording medium 3102, the recording unit 3108 reads the attribute information 3201 that has been stored in the received data record/judging unit 3103 corresponding to the recorded digital data, and writes the read attribute information 3201 on the recording medium 3102. In addition, the recording unit 3108 informs the received data record/judging unit 3103 of the completion of the copying, and informs the accounting information recording unit 3109 of the title code of the recorded digital data.

[0176] When informed of the title code 3204 by the recording unit 3108, the accounting information recording unit 3109 reads the recording charge 3205 of the attribute information 3201 corresponding to the title code 3204 that has been stored in the received data record/judging unit 3103. When finding that the recording charge 3205 must be paid, the accounting information recording unit 3109 records the title code 3204 and the recording charge 3205 on the accounting information recording medium 3110 as the accounting information.

[0177] The accounting information recording medium 3110 is composed of a RAM card and the like. On the accounting information recording medium 3110, the accounting information of digital data is recorded by the accounting information recording unit 3109 that has been downloaded on the recording medium 3102.

[0178] When receiving an inquiry of a charge from the accounting center (not illustrated) via the communication unit 3101, the accounting unit 3111 reads outstanding accounting information that has been recorded on the accounting information recording medium 3110, and informs the communication unit 3101 of the read outstanding accounting information. After informing the communication unit 3101 of the outstanding accounting information, the accounting unit 3111 records a flag indicating that the accounting center has been informed of outstanding accounting information (indicating settlement) on the accounting information recording medium 3110.

[0179] Here, an explanation of operations in the present embodiment will be given with reference to the flowchart in Fig. 19.

[0180] The received data record/judging unit 3103 awaits an indication to record digital data from the user (step s3402), and judges whether it is permitted to copy the designated digital data on referring to the attribute information 201 (step s3404). When it is not permitted to copy the digital data, the received data record/judging unit 3103 has the display unit 3104 indicate that the copying is not permitted (step s3406) to complete the processing.

[0181] When it is permitted to copy the digital data, the recording medium inherent information obtaining

unit 3106 obtains the inherent information of the recording medium 3102 that has been recorded in a secure area on the recording medium 3102, and informs the encryption unit 3107 of the obtained inherent information (step s3408).

[0182] The encryption unit 3107 creates an encryption key according to the inherent information and re-encrypts the digital data (step s3410).

[0183] The recording unit 3108 records the encrypted digital data on the recording medium 3102 (step s3412).

[0184] Then, the accounting information recording unit 3109 judges whether the recording charge of the recorded digital data must be paid (step s3414). When the recording charge is free, the processing is completed. When the recording charge must be paid, the accounting information recording unit 3109 records the accounting information on the accounting information recording medium 3110 (step s3416) to complete the processing.

[0185] Fig. 20 shows the structure of a playback apparatus for reproducing digital data that has been recorded on the recording medium 3102 by the digital data recording apparatus.

[0186] The digital data playback apparatus includes a recording medium 3102, an input operation unit 3501, a reproducing information reading unit 3502, a display unit 3503, a recording medium inherent information obtaining unit 3504, a decryption unit 3505, a reproducing unit 3506, an accounting information recording unit 3507, and an accounting information recording medium 3508.

[0187] On the recording medium 3102, digital data that has been re-encrypted in the digital data recording apparatus, the management information 3301, the attribute information 3201, and the inherent information for identifying the recording medium 3102 has been recorded.

[0188] When receiving an instruction to start reproducing, the input operation unit 3501 gives the reproducing information reading unit 3502 an instruction of initial activation. When receiving the designation of a title from the user, the input operation unit 3501 informs the reproducing information reading unit 3502 of the title. Note that not only when initial activation is instructed, but also when the recording medium 3102 is inserted into the digital data playback apparatus, the instruction of automatic playback mode is given to the reproducing information reading unit 3502.

[0189] When receiving the instruction of initial activation, the reproducing information reading unit 3502 reads the attribute information 3201 that has been recorded on the recording medium 3102, and has the display unit 3503 indicate items in the attribute information 3201 such as the titles 3202 and players 3203.

[0190] When receiving the instruction of a piece of music or the instruction of automatic playback mode from the input operation unit 3501, the reproducing

information reading unit 3502 judges whether the maximum number of reproducing 3207 in the attribute information 3201 is equal to or greater than "1". When the maximum number of reproducing 3207 is equal to or greater than "1", the reproducing information reading unit 3502 reads the title code 3204 and encrypted digital data that has been recorded from the recording start address 3302 to the recording end address 3303, and informs the decryption unit 3505 of the read digital data. At this time, the reproducing information reading unit 3502 instructs the recording medium inherent information obtaining unit 3504 to obtain the inherent information, and informs the accounting information recording unit 3507 of the title code 3204 and the charge per reproduction. Then, when the digital data has been read, the reproducing information reading unit 3502 rewrites the maximum number of reproducing 3207, which is an item of the attribute information 3201, by decreasing the value of the maximum number of reproducing 3207 by one. Note that when the maximum number of reproducing 3207 is "no limit", the maximum number of reproducing 3207 is not rewritten.

[0191] When judging that the maximum number of reproducing is less than "1", the reproducing information reading unit 3502 has the display unit 3502 indicate that the digital data cannot be reproduced any more.

[0192] The display unit 3503 is composed of a liquid crystal display and the like, and displays the list of titles that have been read by the reproducing information reading unit 3502 and other information. In addition, when the user designates a title of music data that has been reproduced the maximum number of times, the display unit 3503 indicates that the music data cannot be reproduced any more.

[0193] When instructed by the reproducing information reading unit 3502 to obtain the inherent information, the recording medium inherent information obtaining unit 3504 obtains the inherent information, which is the identifier of the recording medium 3102 from a secure area on the recording medium 3102, and informs the decryption unit 3505 of the obtained inherent information.

[0194] When informed of the inherent information by the recording medium inherent information obtaining unit 3504 and of the encrypted digital data from the reproducing information reading unit 3502, the decryption unit 3505 creates a decryption key according to the inherent information, decrypts the encrypted digital data, and informs the reproducing unit 3506 of the decrypted digital data.

[0195] When informed of the decrypted digital data by the decryption unit 3505, the reproducing unit 3506 decodes the digital data to reproduce music. After the reproducing of the music, the reproducing unit 3506 informs the accounting information recording unit 3507 that the reproducing is finished.

[0196] When informed that the reproducing is fin-

ished by the reproducing unit 3506, the accounting information recording unit 3507 records the title code 3204 and the charge per reproduction 3206 that have been received from the reproducing information reading unit 3502 and the reproducing date as the accounting information on the accounting information recording medium 3508. Note that when the charge per reproduction 3206 is "free", the charge per reproduction 3206 is not recorded.

[0197] The accounting information recording medium 3508 is composed of a RAM card and the like. On the accounting information recording medium 3508, accounting information is recorded by the accounting information recording unit 3507.

[0198] Here, an explanation of operation by the digital data playback apparatus will be given with reference to the flowchart shown in Fig. 21.

[0199] First, the user instructs the start of reproduction using, for instance, a remote control of the input operation unit 3501, and designates a title of music displayed by the display unit 3503. The reproducing information reading unit 3502 regards the designation as a requirement to reproduce the music data (digital data) corresponding to the title (step s3602), and judges whether the maximum number of reproducing 3207 of the music is equal to or greater than "1" on referring to the attribute information 3201 (step s3604). When the maximum number of reproducing 3207 is less than "1", the reproducing information reading unit 3502 has the display unit 3503 indicate that the music data has been reproduced the maximum number of times (step s3606) to complete the processing.

[0200] When the maximum number of reproducing 3207 is equal to or greater than "1", the reproducing information reading unit 3502 reads the encrypted digital data from the recording medium 3102 and informs the decryption unit 3505 of the read digital data (step s3608).

[0201] Meanwhile, the recording medium inherent information obtaining unit 3504 obtains the inherent information from the recording medium 3102 and informs the decryption unit 3505 of the obtained inherent information (step s3610).

[0202] The decryption unit 3505 decrypts the encrypted digital data using the inherent information as the decryption key (step s3612).

[0203] The reproducing unit 3506 decodes the digital data to reproduce and output music (step s3614).

[0204] Then, the accounting information recording unit 3507 judges whether the charge per reproduction 3206 must be paid (step s3616). When the charge per reproduction 3206 is "free", the processing is completed. When the charge per reproduction 3206 must be paid, the accounting information recording unit 3507 records the accounting information on the accounting information recording medium 3508 (step s3618) to complete the processing.

(The Seventh Embodiment)

[0205] Fig. 22 shows the structure of a digital data recording apparatus according to the seventh embodiment of the present invention. The digital data recording apparatus includes a first digital data recording apparatus 3700 and a second digital data recording/playback apparatus 3710.

[0206] The first digital data recording apparatus 3700 includes a first recording medium 3701, a communication unit 3101, a received data primary record/judging unit 3702, a display unit 3104, an input operation unit 3105, a primary recording unit 3703, a received data read/judging unit 3704, an inherent information obtaining unit 3705, an encryption unit 3706, an accounting information recording unit 3109, an accounting information recording medium 3110, and an accounting unit 3111. The first digital data recording apparatus is realized by a PC.

[0207] The second digital data recording/playback apparatus includes an inherent information obtaining/transfer unit 3707, a secondary recording unit 3708, a second recording medium 3709, an input operation unit 3501, a reproducing information reading unit 3502, a display unit 3503, a decryption unit 3505, a reproducing unit 3506, an accounting information recording unit 3507, and an accounting information recording medium 3508.

[0208] Note that the elements of the first digital data recording apparatus 3700 and the second digital data recording/playback apparatus in the seventh embodiment that are the same in the digital data recording apparatus and the digital data playback apparatus in the sixth embodiment have the same reference numbers and explanations of the elements are not given below.

[0209] First, an explanation of the first digital data recording apparatus 3700 will be given. The first digital data recording apparatus 3700 is different from the digital data recording apparatus in the sixth embodiment in the points that the first recording medium 3701 is fixed in the first digital data recording apparatus 3700 and digital data that has been recorded on the first recording medium 3701 is output after being encrypted for secondary recording.

[0210] The first recording medium 3701 is composed of a rewriteable recording element such as a hard disk that is fixed in the first digital data recording apparatus 3700. On the first recording medium 3701, digital data (music data) that has been received by the communication unit 3101 and the management information of the digital data are recorded by the primary recording unit 3703.

[0211] The received data primary record/judging unit 3702 writes attribute data attached to the digital data that has been received by the communication unit 3101 in a storage area in an EEPROM. One example of attribute information that is received in the present embodiment is shown in Fig. 23. Attribute information

3601 is different from the attribute information 3201 in the sixth embodiment in the point that secondary recording charges 3802, copy permission (primary) 3803, and copy permission (secondary) are indicated.

[0212] The attribute information 3801 shows that neither of the primary and secondary copying is not permitted and only listening in real time is permitted for a title "music E" having title code "song05".

[0213] When instructed secondary recording of music by the user, the received data primary record/judging unit 3702 judges whether primary recording is permitted for the music on referring to an item in the attribute information 3801, copy permission (primary) 3803. When the primary recording is not permitted, the received data primary record/judging unit 3702 has the display unit 3104 indicate that the primary recording for the music is not permitted. When the primary recording is permitted, the received data primary record/judging unit 3702 informs the primary recording unit 3703 of the digital data of the music. Other functions of the received data primary recording judging unit are the same as of the received data record/judging unit 3103.

[0214] The primary recording unit 3703 records the received digital data on the first recording medium 3701. At this time, the management information is also written as in the case of the recording unit 3108 in the sixth embodiment. Note that while an encryption key is created according to the inherent information of the recording medium 3102 to re-encrypt digital data in the sixth embodiment, the digital data is not re-encrypted since the first recording medium 3701 is not removable from the first digital data recording apparatus 3700, i.e., is not used in another apparatus in the present embodiment.

[0215] In addition, when the digital data has been recorded on the first recording medium 3701, the primary recording unit 3703 informs the received data read/judging unit 3704 of the title code 3805 of the recorded digital data.

[0216] When informed of the title code 3805 by the primary recording unit 3703, the received data read/judging unit 3704 judges whether the secondary recording of the music is permitted on referring to the copy permission (secondary) 3804 in the attribute information 3801 in the received data primary record/judging unit 3702. When the secondary recording is not permitted, or when the permitted number of times is less than "1", the received data read/judging unit 3704 has the display unit 3104 indicate that the secondary recording is not permitted for the music.

[0217] When the secondary recording is permitted, the received data read/judging unit 3704 refers to the management information (refer to Fig. 18), reads the digital data of the title code that has been recorded on the first recording medium 3701. The received data read/judging unit 3704 informs the encryption unit 3706 of the digital data, and instructs the inherent information

obtaining unit 3705 to obtain inherent information.

[0218] When having read the digital data, the received data read/judging unit 3704 decreases the number of times of the copy permission (secondary) 3804 by "1" in the attribute information 3701 that has been stored in the received data primary record/judging unit 3702. For instance, "only once" is changed to "not permitted", and "permitted" is not written since the number of times is not limited.

[0219] Note that after notifying the encryption unit 3706 of the digital data, the received data read/judging unit 3704 reads the attribute information that has been stored in the received data primary record/judging unit 3702.

[0220] When instructed to obtain inherent information by the received data read/judging unit 3704, the inherent information obtaining unit 3705 requests the inherent information obtaining/transfer unit 3707 in the second digital data recording/playback apparatus 3710 that is connected to the first digital data recording apparatus 3700 to transmit the inherent information. When informed of the inherent information by the inherent information obtaining/transfer unit 3707, the inherent information obtaining unit 3705 informs the encryption unit 3706 of the inherent information.

[0221] The encryption unit 3706 creates an encryption key according to the inherent information that has been transferred from the inherent information obtaining unit 3705, encrypts the digital data that has been transferred from the received data read/judging unit 3704, and transmits the encrypted digital data to the secondary recording unit 3708 in the second digital data recording/playback apparatus 3710. After the transmission of the encrypted digital data, the encryption unit 3706 transmits the received attribute information.

[0222] Here, an explanation of the second digital data recording/playback apparatus 3710 will be given. The second digital data recording/playback apparatus 3710 is realized by, for instance, a portable headphone stereo apparatus. The second recording medium 3709 is composed of a semiconductor memory such as an IC card that is removable from the second digital data recording/playback apparatus 3710.

[0223] When required to transmit the inherent information by the inherent information obtaining unit 3705 in the first digital data recording apparatus 3700, the inherent information obtaining/transfer unit 3707 obtains the medium identification information inherent in the second recording medium 3709 that is recorded on the second recording medium 3709 in advance and the apparatus identification information inherent in the second digital data recording/playback apparatus 3710, and informs the inherent information obtaining unit 3705 of the obtained medium identification information and apparatus identification information. Meanwhile, when instructed to inform inherent information by the reproducing information reading unit 3502, the inherent information obtaining/transfer unit 3707 informs the

decryption unit 3505 of the obtained medium identification information and apparatus identification information.

[0224] When receiving the encrypted digital data and the attribute information that has been output from the encryption unit 3706 in the first digital data recording apparatus 3700, the secondary recording unit 3708 records the received encrypted digital data and the attribute information on the second recording medium 3709. In addition, the secondary recording unit 3708 records the management information 3301 shown in Fig. 18 on the second recording medium 3709. The decryption unit 3505 creates a decryption key according to the medium identification information and the apparatus identification information that have been transferred from the inherent information obtaining/transfer unit 3707, and decrypts the encrypted digital data that has been transferred from the reproducing information reading unit 3502 using the created decryption key. Note that other parts of the structure of the second digital data recording/playback apparatus 3710 are almost the same as the digital data playback apparatus in the sixth embodiment.

[0225] Here, an explanation will be given when the second recording medium 3709 is composed of an IC card that is fixed in the second digital data recording/playback apparatus 3710. In this case, since the second recording medium 3709 is only used in the second digital data recording/playback apparatus 3710, the inherent information obtaining/transfer unit 3707 obtains no medium identification information and informs the inherent information obtaining unit 3705 of the apparatus identification information that the inherent information obtaining/transfer unit 3707 stores. Meanwhile, the inherent information obtaining/transfer unit 3707 informs the decryption unit 3505 at the apparatus identification information.

[0226] As has been described, it depends on whether the second recording medium 3709 in the second digital data recording/playback apparatus 3710 is removable that an encryption key for encrypt digital data is created according to the combination of the medium identification information and the apparatus identification information or the apparatus identification information. By doing so, unauthorized duplication and reproduction of digital data can be prevented.

[0227] Here, an explanation of operations in the seventh embodiment will be given with reference to the flowchart shown in Fig. 24.

[0228] First, the received data primary record/judging unit 3702 awaits an instruction of the secondary recording of digital data from the input operation unit 3105 (step s3902), and judges whether the primary recording of the digital data is permitted on referring to the attribute information 3801 (step s3904). When the primary recording is not permitted, the received data primary record/judging unit 3702 has the display unit 3104 indicate that the primary recording is not permitted

(step s3906) to complete the processing.

[0229] When the primary recording is permitted, the received data primary record/judging unit 3702 informs the primary recording unit 3703 of the digital data. The primary recording unit 3703 records the digital data and the management information on the first recording medium 3701 (step s3908).

[0230] Next, the accounting information recording unit 3109 judges whether the primary recording is charged (step s3910), and records the accounting information on the accounting information recording medium 3110 when the primary recording is charged (step s3912).

[0231] Then, the received data read/judging unit 3704 judges whether the secondary recording of the digital data that has been recorded on the first recording medium 3701 is permitted on referring to the attribute information 3801 that has been stored in the received data primary record/judging unit 3702 (step s3914). When the secondary recording is not permitted, the received data read/judging unit 3704 has the display unit 3104 indicate that the secondary recording is not permitted (step s3916) to complete the processing.

[0232] When the secondary recording is permitted, the received data read/judging unit 3704 reads the digital data from the first recording medium 3701, informs the encryption unit 3706 of the read digital data, and instructs the inherent information obtaining unit 3705 to obtain the inherent information from the second digital data recording/playback apparatus 3710. The inherent information obtaining unit 3705 obtains the inherent information and informs the encryption unit 3706 of the obtained inherent information (step s3918). The encryption unit 3706 creates an encryption key according to the received inherent information (step s3920), encrypts the received digital data, and outputs the encrypted digital data to the secondary recording unit 3708 in the second digital data recording/playback apparatus 3710.

[0233] The secondary recording unit 3708 records the encrypted digital data, the attribute information, and the management information on the secondary recording medium 3709 (step s3922).

[0234] The accounting information recording unit 3109 judges whether the secondary recording is charged (step s3924), and records the accounting information on the accounting information recording medium 3110 when the secondary recording is charged (step s3926) to complete the processing.

[0235] Note that operations in reproducing the digital data by the second digital data recording/playback apparatus 3710 are almost the same as operations by the digital data playback apparatus in the sixth embodiment, so that no explanation will be given.

(Another Example)

[0236] While the digital data is encrypted in the seventh embodiment using the encryption key according to

the combination of the apparatus identification information of the second digital data recording/playback apparatus 3710 and the medium identification information of the second recording medium 3709 when the second recording medium 3709 is removable, the form of encryption is designated by the user (it is designated by the user whether the encryption key is created according to only the medium identification information or the combination of the medium identification information and the apparatus identification information) to increase the degree of freedom of usage patterns in this another example of the seventh embodiment. More specifically, when reproduced with the second digital data recording/playback apparatus 3710, the digital data of music that has been recorded on the second recording medium 3709 is encrypted using the medium identification information and the apparatus identification information at the time of recording. When reproduced with another digital data playback apparatus (an apparatus that decrypts encrypted digital data using the medium identification information as the decryption key), the digital data is encrypted using the medium identification information at the time of recording. As a result, the form of encryption can be selected according to the usage pattern.

[0237] On the other hand, the secondary recording charges are determined according to the degree of freedom of usage pattern to protect the copyright.

[0238] Here, an explanation of the structure of the first digital data recording apparatus and the second digital data recording/playback apparatus in the other example of the seventh embodiment will be given. Note that the functions of the first digital data recording apparatus and the second digital data recording/playback apparatus in this example are realized by adding a few functions to those of the first digital data recording apparatus 3700 shown in Fig. 22. As a result, an explanation of only the parts of structure that are different from the seventh embodiment will be given with reference to Fig. 22 that has been used in the explanation of the seventh embodiment.

[0239] Fig. 25 shows part of attribute information 31001 that is stored in the received data primary record/judging unit 3702. The attribute information 31001 is different from the attribute information 3801 shown in Fig. 23 in the contents of the secondary recording charges 3802 and secondary recording charges 31002.

[0240] A secondary recording charge 31002 depends on whether the encryption key used in the encryption of digital data is created according to the medium identification information (medium ID) 31003, the apparatus identification information (apparatus ID) 31004, or the combination of the medium identification information and the apparatus identification information. When the encryption key has been created according to the medium identification information 31003, the music data can be reproduce by using the second recording

medium 3709 in another apparatus and the degree of freedom of the user is increased. As a result, the secondary recording charge (secondary replication charge) is higher than when the encryption key has been created according to the apparatus identification information 31004 and the combination of the medium identification information and the apparatus identification information 31005. By doing so, the replication charge is determined according to the usage pattern.

[0241] When informed of the apparatus identification information and the medium identification information from the inherent information obtaining/transfer unit 3707, the inherent information obtaining unit 3705 has the display unit 3104 indicate whether the second recording medium 3709 is used in the second digital data recording/playback apparatus 3710 or in another apparatus to await the user selection.

[0242] The user designates the second digital data recording/playback apparatus 3710 or another apparatus using the input operation unit 3105, i.e., to create the encryption key according to the medium identification information or to create the encryption key according to the combination of the medium identification information and the apparatus identification information.

[0243] The input operation unit 3105 informs the received data primary record/judging unit 3702 of the user's designation.

[0244] When informed by the input operation unit 3105 that another apparatus is to be used, the received data primary record/judging unit 3702 informs the accounting information recording unit 3109 that the secondary recording charge 31002 is determined according to the encryption key that is created using the medium identification information 31003. On the other hand, when informed that only the second digital data recording/playback apparatus is to be used, the received data primary record/judging unit 3702 informs the accounting information recording unit 3109 that the secondary recording charge 31002 is determined according to the encryption key that is created using the combination of the medium identification information and the apparatus identification information 31005.

[0245] When informed by the input operation unit 3105 that another apparatus is to be used, the inherent information obtaining unit 3705 informs the encryption unit 3706 of only the medium identification information 31003. On the other hand, when informed by the input operation unit 3105 that only the second digital data recording/playback apparatus 3710 is to be used, the inherent information obtaining unit 3705 informs the encryption unit 3706 of the combination of the medium identification information and the apparatus identification information 31005.

[0246] When informed by the encryption unit 3706 that the encrypted digital data has been transmitted to the secondary recording unit 3708, the accounting information recording unit 3109 refers to the secondary recording charge 31002 in the attribute information

31001 that has been informed of by the received data primary record/judging unit 3702, and records the accounting information on the accounting information recording medium 3110.

[0247] Note that it is needless to say that, in this example, when the second recording medium 3709 is a removable DVD-RAM, the encryption key can be created only according to the identification information inherent to the DVD-RAM, the digital data can be re-encrypted using the created encryption key, and the re-encrypted digital data can be recorded as in the case of the sixth embodiment.

[0248] Meanwhile, operations in this example are essentially the as in the seventh embodiment, so that no explanation will be given.

[0249] Note that it is possible to suppose that the accounting information recording media 3110 and 3508 are realized by IC cards, for instance, and the digital data is not recorded and reproduced without setting the IC cards in the sixth and seventh embodiments and in the example.

[0250] In addition, while the digital data that is received by the communication unit 3110 has been supposed to be music data in the sixth and seventh embodiments and in the example, the digital data can be video data, audio data, character data, and the combination of them.

[0251] While the structures of the digital data recording apparatus, the digital data playback apparatus, and the digital data recording/playback apparatus are shown in Figs. 16, 20, and 22, it is possible to record a program realizing the functions of the elements on a computer-readable recording medium such as a floppy disk, to use the computer-readable recording medium in a digital data recording/playback apparatus that has no function of protecting copyrights, and to have the digital data recording/playback apparatus has a function of protect copyrights.

[0252] Although the present invention has been fully described by way of examples with reference to the accompanying drawings, it is to be noted that various changes and modifications will be apparent to those skilled in the art. Therefore, unless such changes and modifications depart from the scope of the present invention, they should be construed as being included therein.

INDUSTRIAL USE POSSIBILITY

[0253] As has been described the digital data recording apparatus according to the present invention protects copyrights, reduces the cost of playback apparatus. As a result, the digital data recording apparatus is suitable for recording electronically-distributed digital data that has been encrypted in different encryption systems, especially for recording electronically-distributed music data.

Claims

1. A digital data recording apparatus for recording digital data on a recording medium, comprising:

communication means for receiving encrypted digital data via a digital network;

decryption means for decrypting the encrypted digital data that has been received by the communication means;

encryption means including a plurality of encryption units that re-encrypt decrypted digital data in encryption systems having different security levels;

recording means for recording digital data that has been re-encrypted by the encryption means on the recording medium; and

a controller for controlling the decryption means and the encryption means, wherein the controller has one of the plurality of encryption units re-encrypt the digital data that has been decrypted by the decryption means.

2. The digital data recording apparatus according to Claim 1, wherein

the digital data that has been recorded on the recording medium is reproduced by a playback apparatus,

the encryption means includes:

a first encryption unit for re-encrypting digital data using an encryption key that has been created according to identification information of the recording medium; and

a second encryption unit for re-encrypting digital data using an encryption key that has been created according to identification information of the playback apparatus; and

the controller judges whether the recording medium is removable from the playback apparatus, has the first encryption unit re-encrypt the decrypted digital data when the recording medium is removable from the playback apparatus, and has the second encryption unit re-encrypt the decrypted digital data when the recording medium is not removable from the playback apparatus.

3. The digital data recording apparatus according to Claim 1, further comprising accounting means for conducting an accounting process via the digital network, wherein

the controller determines an accounting value according to an encryption unit that has re-encrypted the decrypted digital data, and controls the accounting means so that the controller conducts the accounting process according

to the determined accounting value.

4. The digital data recording apparatus according to Claim 3, wherein

the digital data that has been recorded on the recording medium is reproduced by a playback apparatus,

the encryption means includes:

a first encryption unit for re-encrypting digital data using an encryption key that has been created according to identification information of the recording medium; and

a second encryption unit for re-encrypting digital data using an encryption key that has been created according to identification information of the playback apparatus; and

the controller judges whether the recording medium is removable from the playback apparatus, has the first encryption unit re-encrypt the decrypted digital data when the recording medium is removable from the playback apparatus, and has the second encryption unit re-encrypt the decrypted digital data when the recording medium is not removable from the playback apparatus.

5. The digital data recording apparatus according to Claim 4, wherein the controller prohibits the decryption means from decrypting the encrypted digital data when the encryption means fails to create any encryption key.

6. The digital data recording apparatus according to Claim 1, wherein the security levels of the encryption systems in which the plurality of encryption units re-encrypt decrypted digital data are lower than security levels of encryption systems in which encrypted digital data that are to be received by the communication means have been encrypted.

7. The digital data recording apparatus according to Claim 1, wherein

the encrypted digital data that is received by the communication means has been encrypted in one of encryption systems having different security levels and includes attribute information that indicates the encryption system, the decryption means includes a plurality of decryption units that decrypt encrypted digital data that have been encrypted in the encryption systems, and the controller judges the encryption system in which the encrypted digital data has been encrypted according to the attribute information, and controls the decryption means so that one of the plurality of decryption units corre-

sponding to the judged encryption system decrypts the encrypted digital data.

8. The digital data recording apparatus according to Claim 7, further comprising accounting means for conducting an accounting process via the digital network, wherein

the controller determines an accounting value according to a decryption unit that has decrypted the encrypted digital data and an encryption unit that has re-encrypted the decrypted digital data, and controls the accounting means so that the controller conducts the accounting process according to the determined accounting value.

9. A digital data recording method of recording digital data on a recording medium, comprising:

a communication step for receiving encrypted digital data via a digital network;
a decryption step for decrypting the encrypted digital data that has been received at the communication step;
an encryption step for re-encrypting decrypted digital data in one of a plurality of encryption systems having different security levels; and
a recording step for recording digital data that has been re-encrypted at the encryption step on the recording medium.

10. The digital data recording method according to Claim 9, wherein

the encrypted digital data that is received at the communication step has been encrypted in one of encryption systems having different security levels and includes attribute information that indicates the encryption system, the digital data recording method, further comprising a judging step for judging one of the plurality of encryption systems according to the attribute information, wherein the decryption step decrypts the encrypted digital data according to the judgement at the judging step.

11. A computer-readable recording medium that is applied to a digital data recording apparatus for recording digital data on a first recording medium, the computer-readable recording medium storing a program that has a computer execute steps:

a communication step for receiving encrypted digital data via a digital network;
a decryption step for decrypting the encrypted digital data that has been received at the com-

munication step;

an encryption step for re-encrypting decrypted digital data in one of a plurality of encryption systems having different security levels; and
a recording step for recording digital data that
has been re-encrypted at the encryption step
on the recording medium.

5

12. The computer-readable recording medium according to Claim 11, wherein

10

the encrypted digital data that is received at the communication step has been encrypted in one of encryption systems having different security levels and includes attribute information that indicates the encryption system,
the digital data recording method, further comprising a judging step for judging one of the plurality of encryption systems according to the attribute information, wherein
the decryption step decrypts the encrypted digital data according to the judgement at the judging step.

15

20

25

30

35

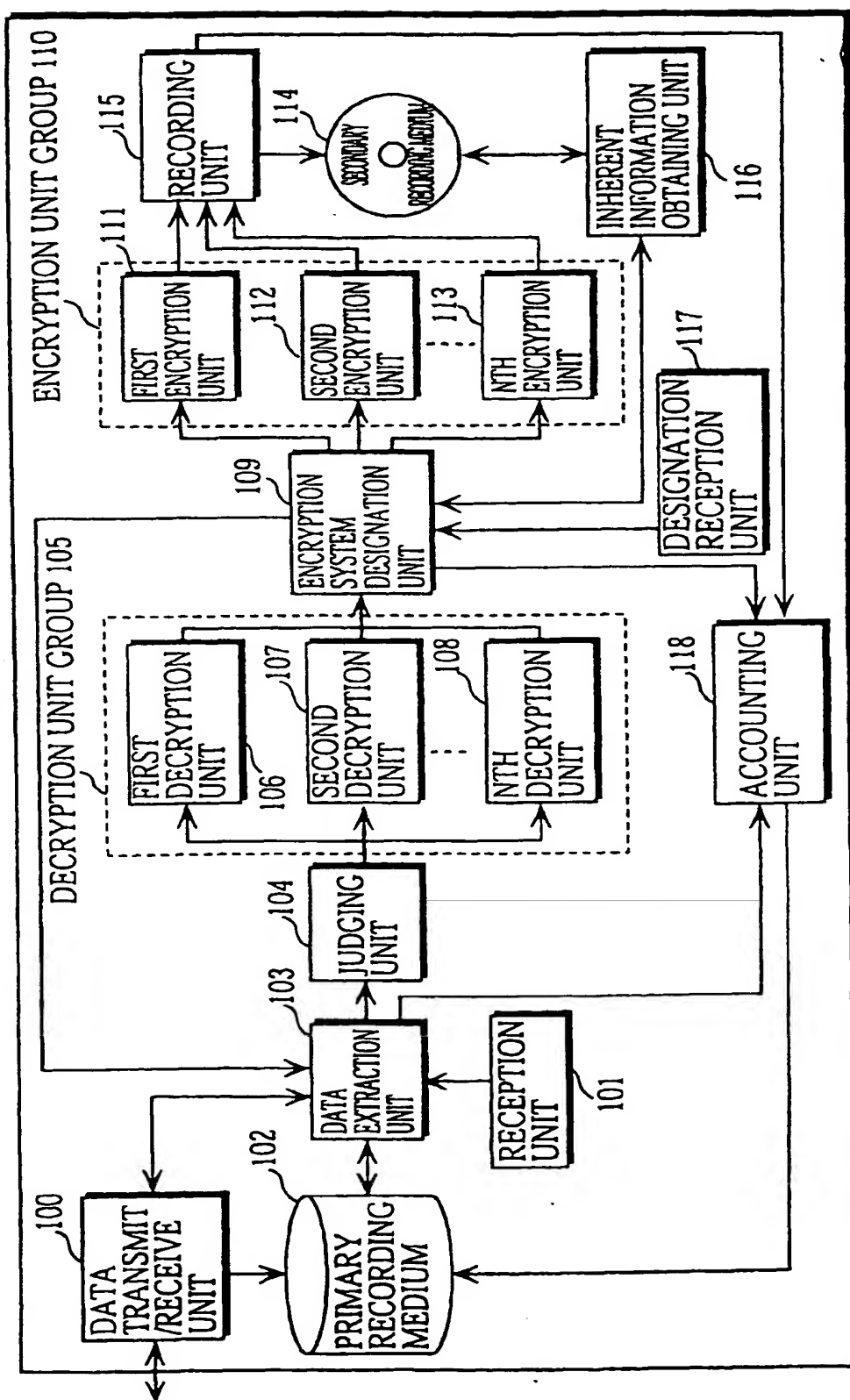
40

45

50

55

FIG. 1



DIGITAL DATA RECORDING APPARATUS

FIG. 2

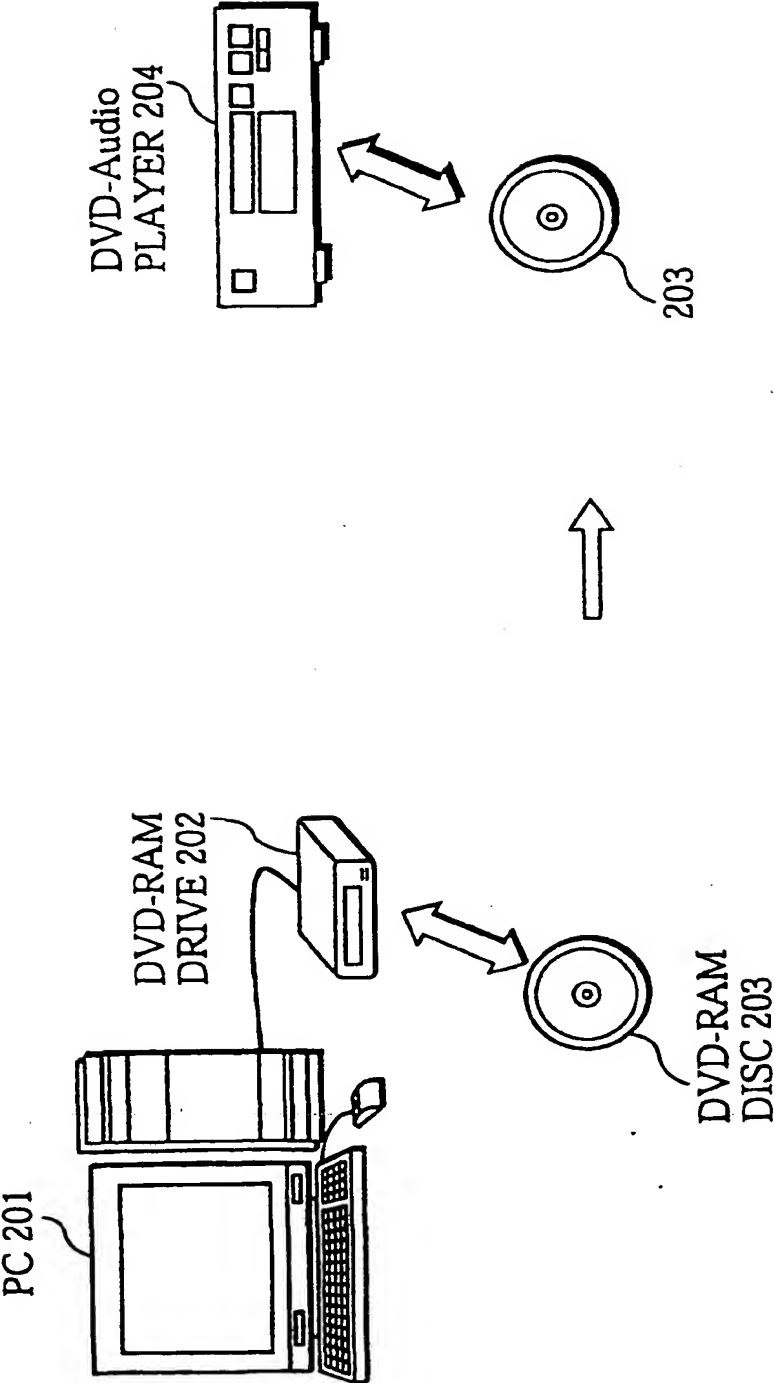


FIG. 3

TITLE	SINGER	TIME	PRICE
Song1	SingerA	4'20"	¥100
Song2	SingerB	3'53"	¥50
Song3	SingerC	4'48"	¥75
Song4	SingerD	4'06"	¥100
:	:	:	:
:	:	:	:

FIG. 4

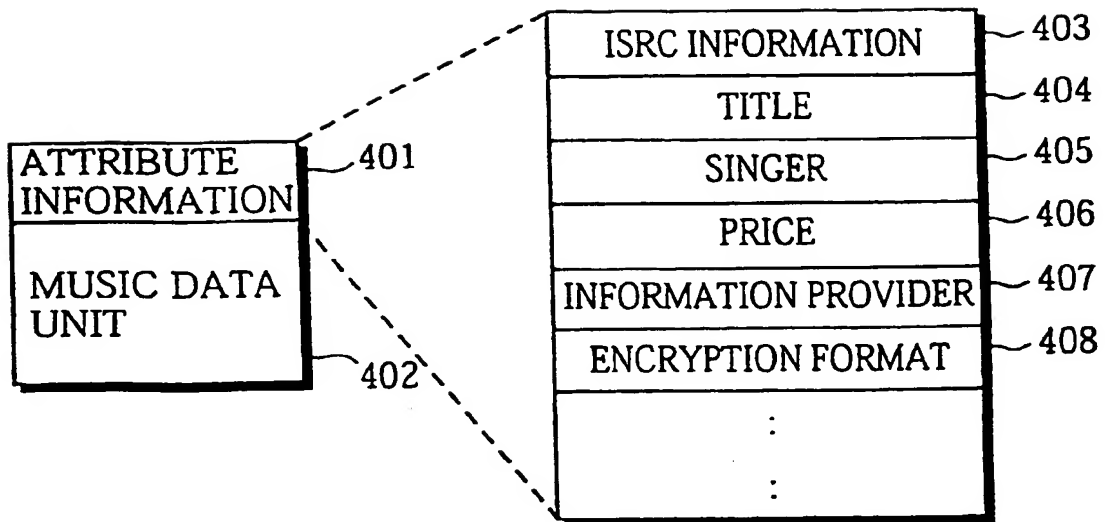


FIG. 5

TITLE	SINGER	TIME	PRICE(1)	PRICE(2)
Song1	SingerA	4'20"	¥100	¥70
Song2	SingerB	3'53"	¥50	¥35
Song3	SingerC	4'48"	¥75	¥50
Song4	SingerD	4'06"	¥100	¥100
:	:	:	:	:
:	:	:	:	:

FIG. 6

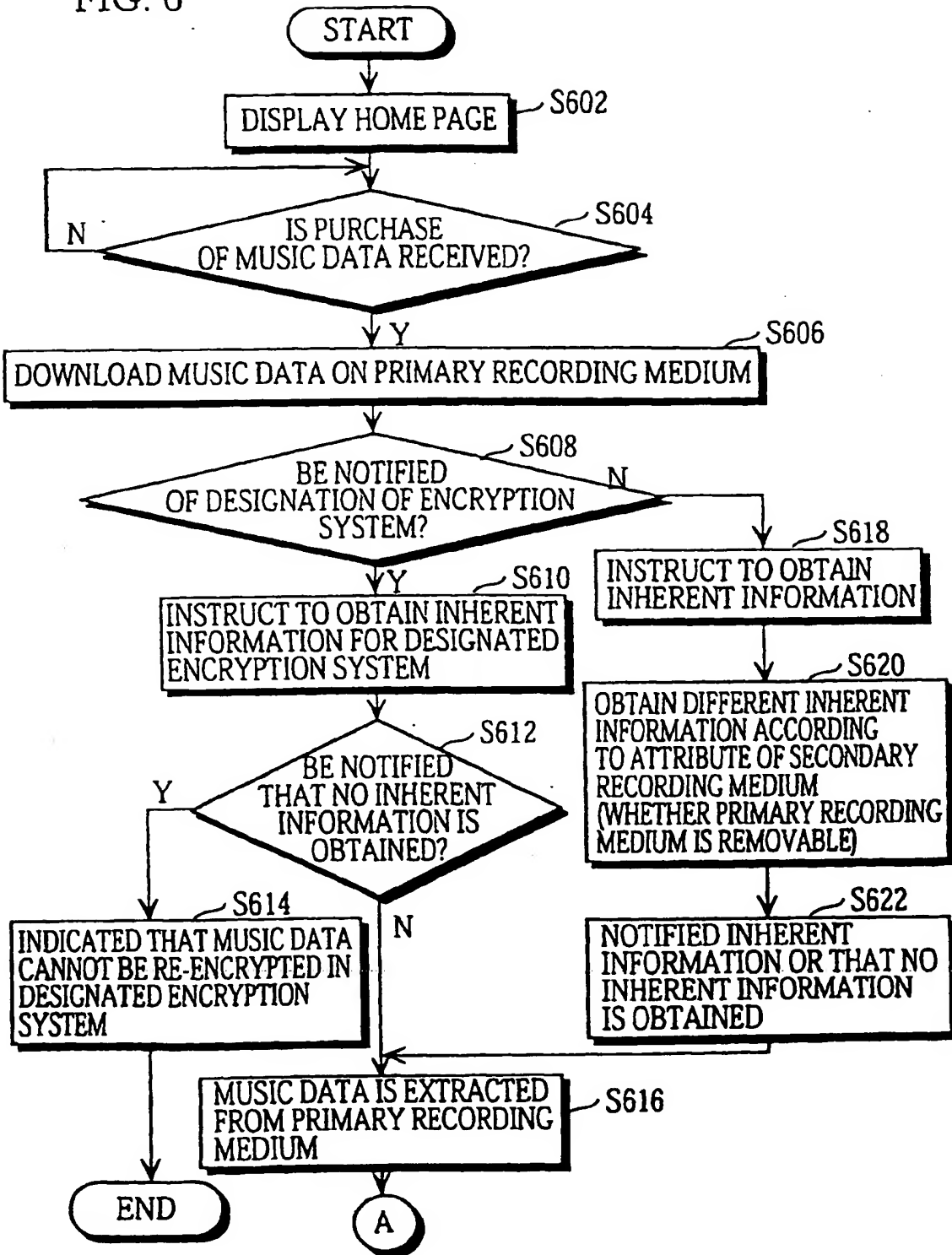


FIG. 7

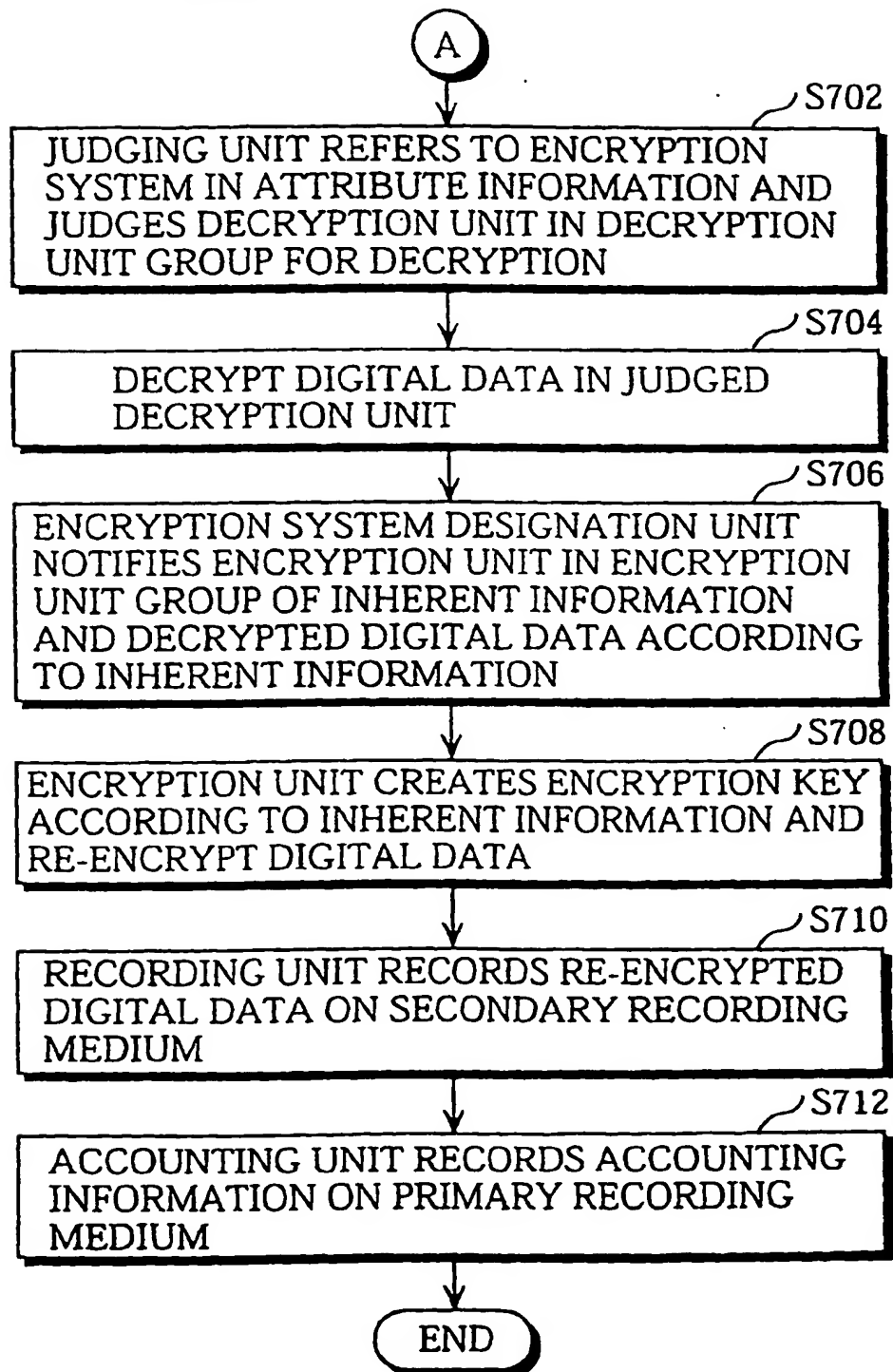


FIG. 8

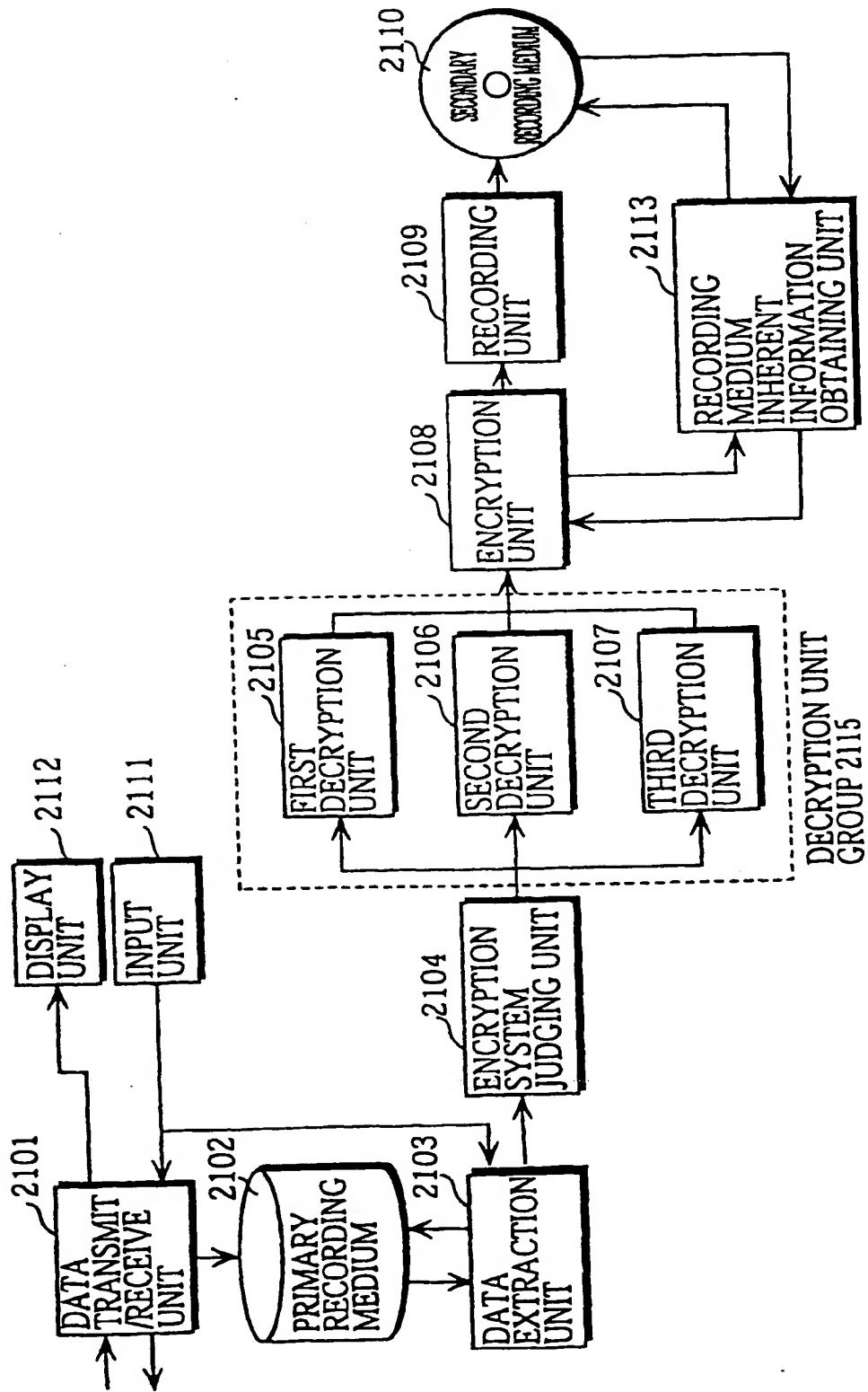


FIG. 9

TITLE	TITLE CODE	SINGER	DATA SOURCE
TITLE A	song01	A	www. song/song01
TITLE B	song02	B	www. song/song02
TITLE C	song03	C	www. song/song03
TITLE D	song04	D	www. song/song04
TITLE E	song05	E	www. song/song05

FIG. 10

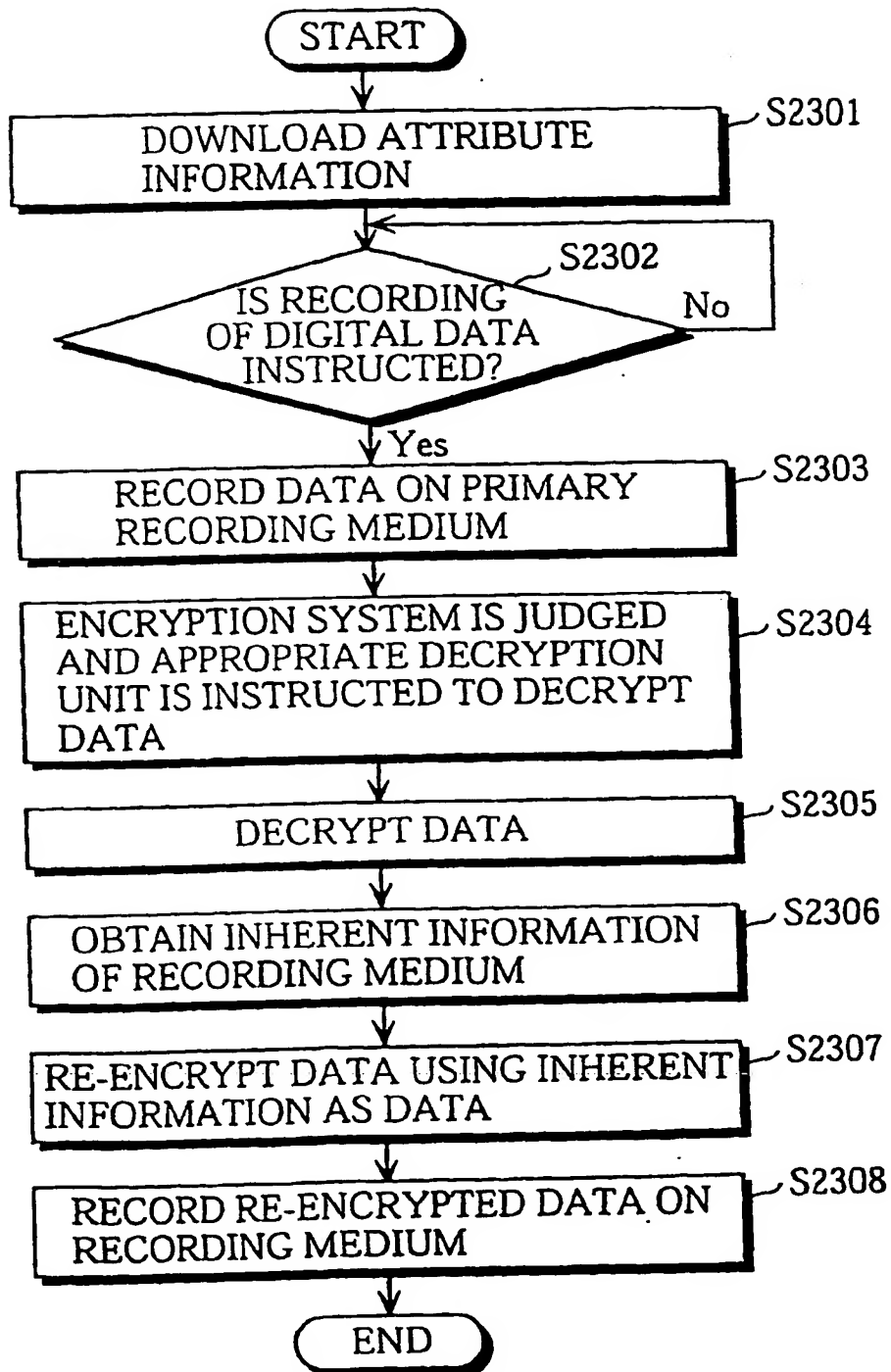


FIG. 11

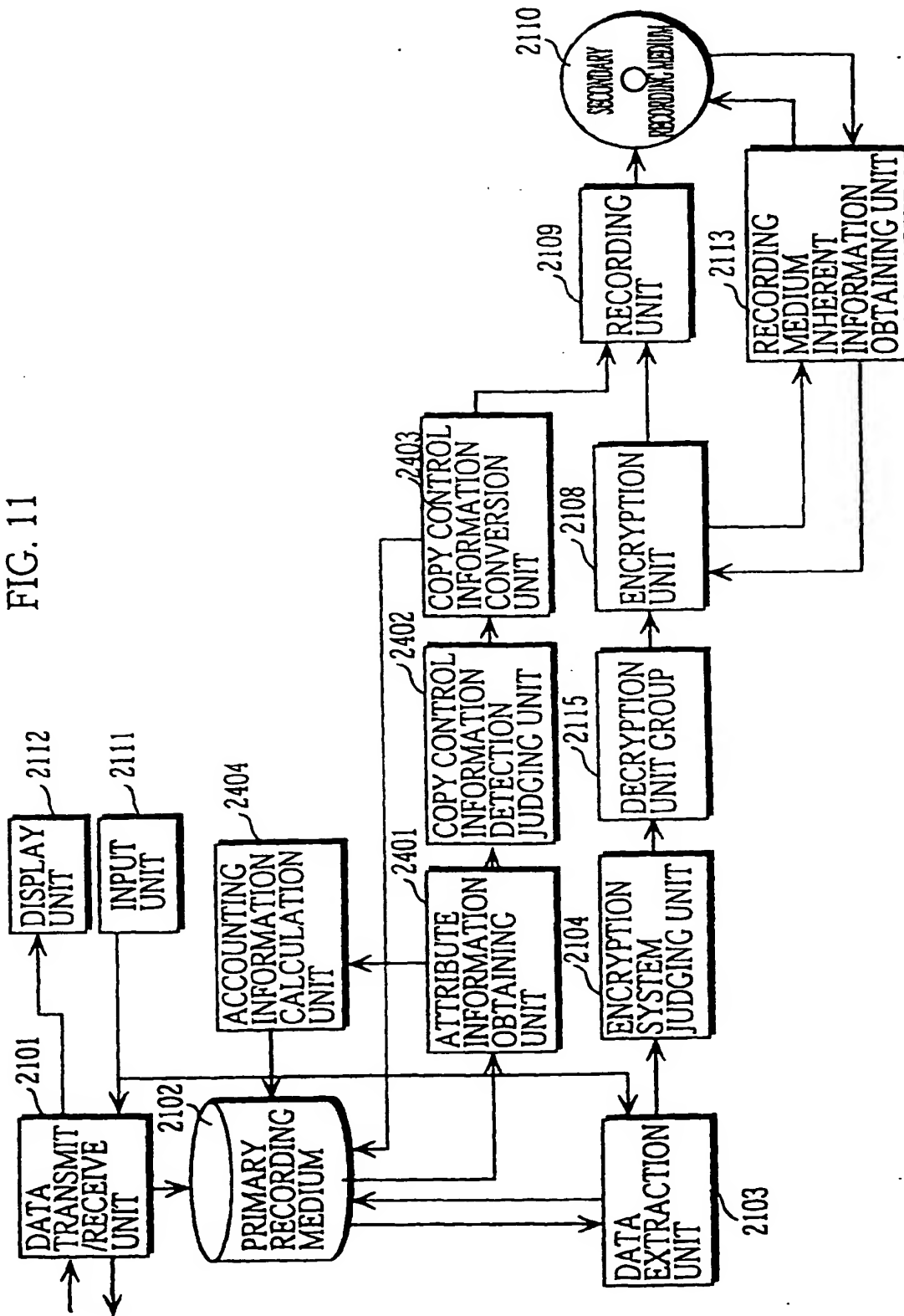


FIG. 12

2201		2202		2203	2204		2501	2502	
TITLE	TITLE CODE	SINGER	DATA SOURCE	COPY CONTROL INFORMATION	PRICE				
TITLE A	song01	A	www. song/song01	NO RECOPYING	¥100				
TITLE B	song02	B	www. song/song02	NO LIMIT	¥10				
TITLE C	song03	C	www. song/song03	NO RECOPYING	¥0				
TITLE D	song04	D	www. song/song04	NO RECOPYING	¥30				
TITLE E	song05	E	www. song/song05	COPYING TWICE	¥10				

FIG. 13

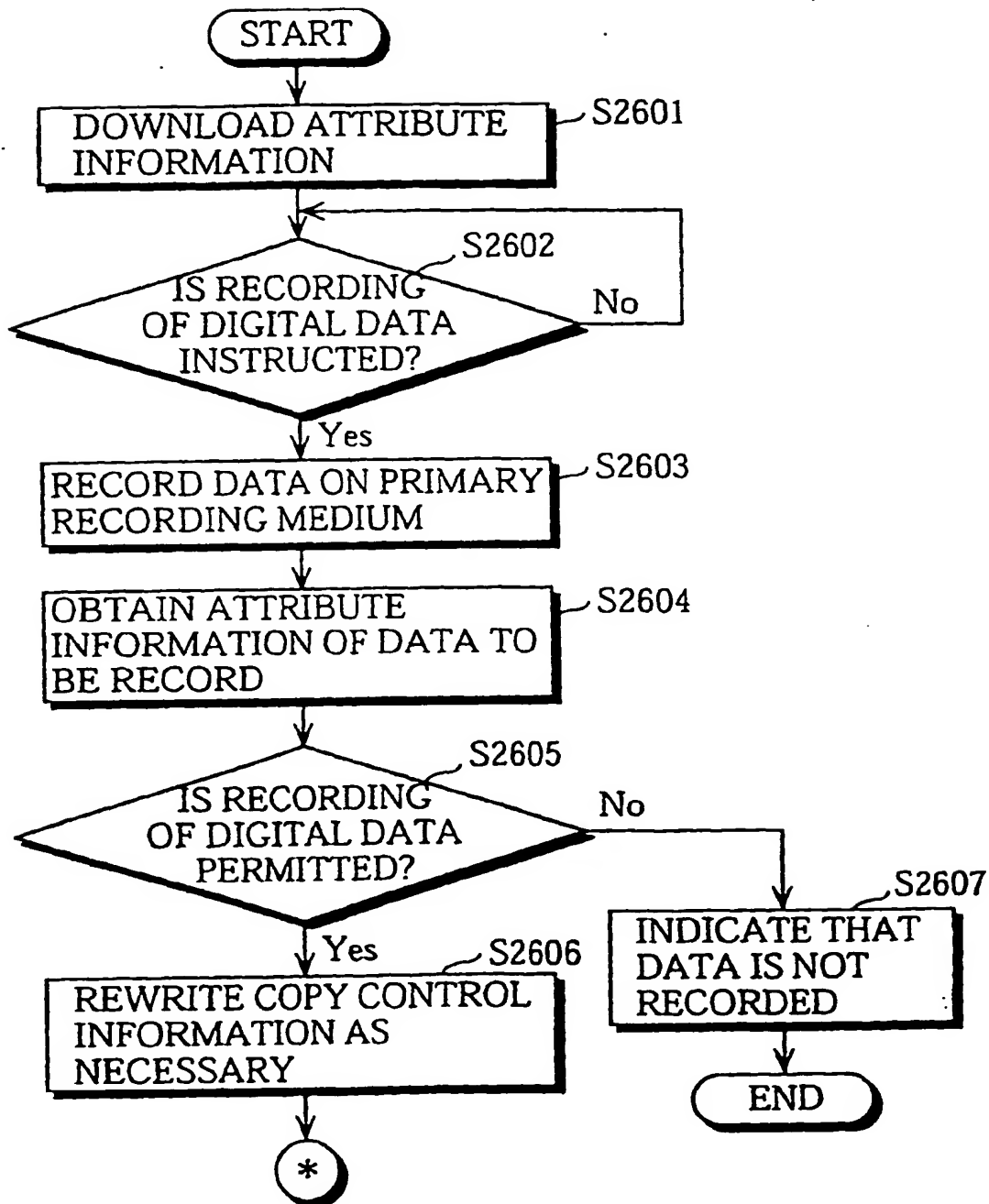


FIG. 14

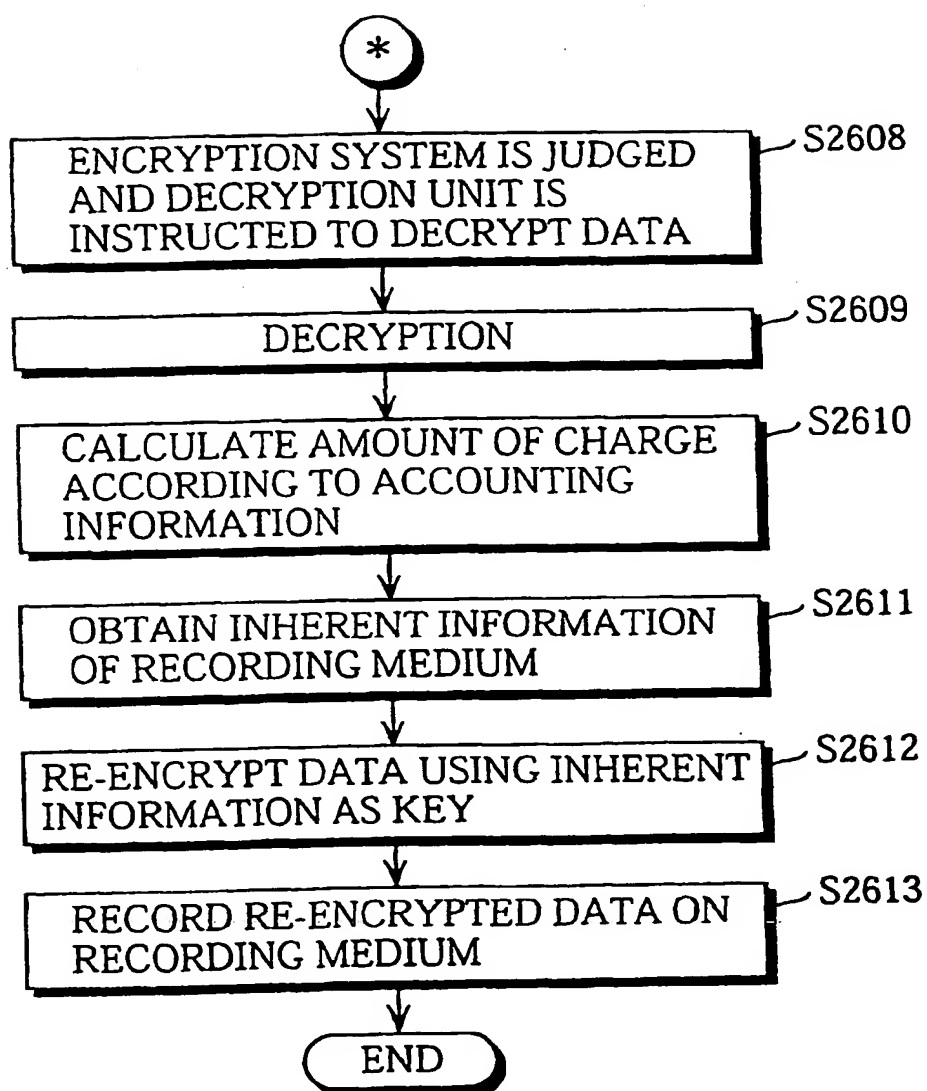
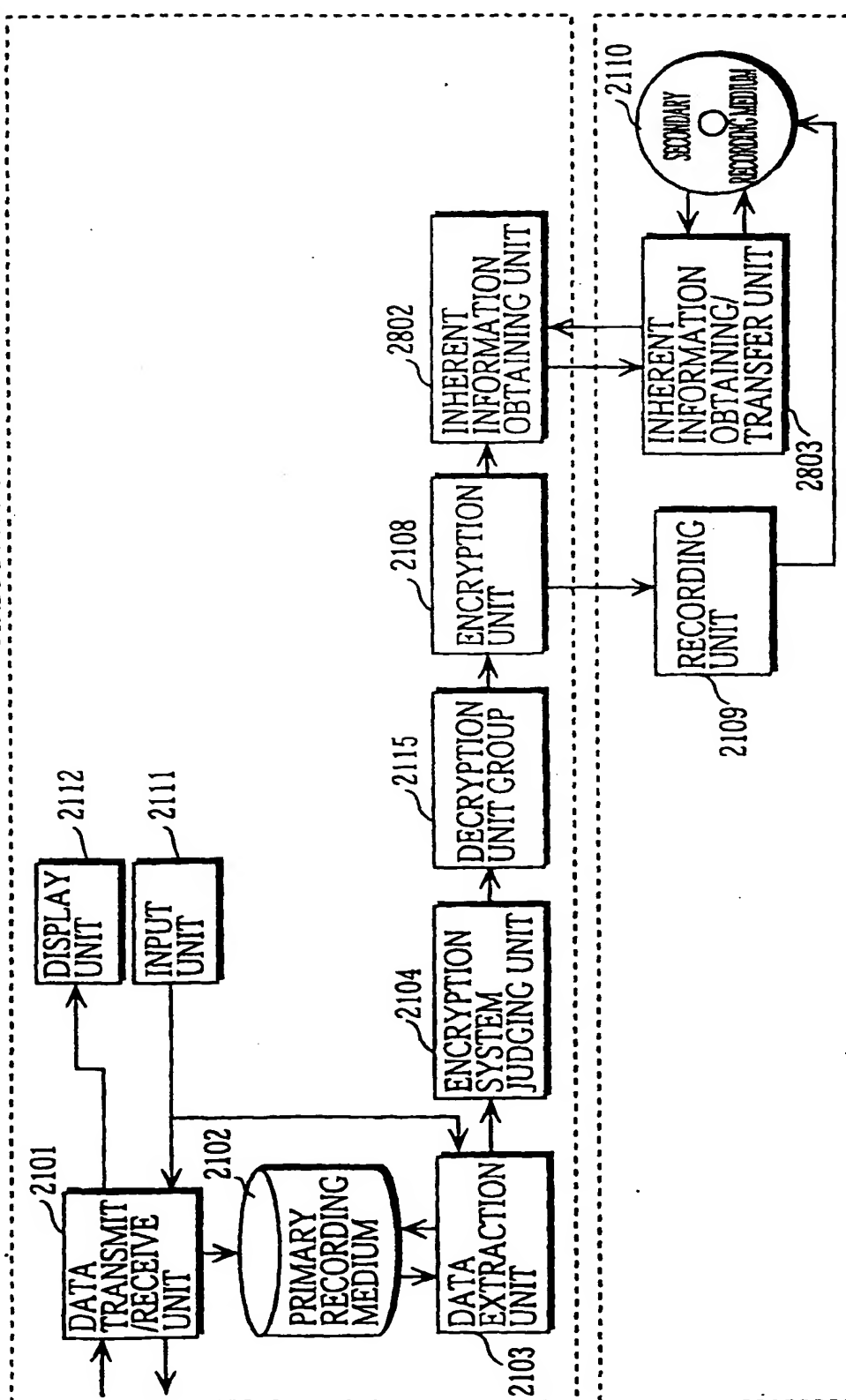


FIG. 15

FIRST DIGITAL DATA RECORDING APPARATUS 2800



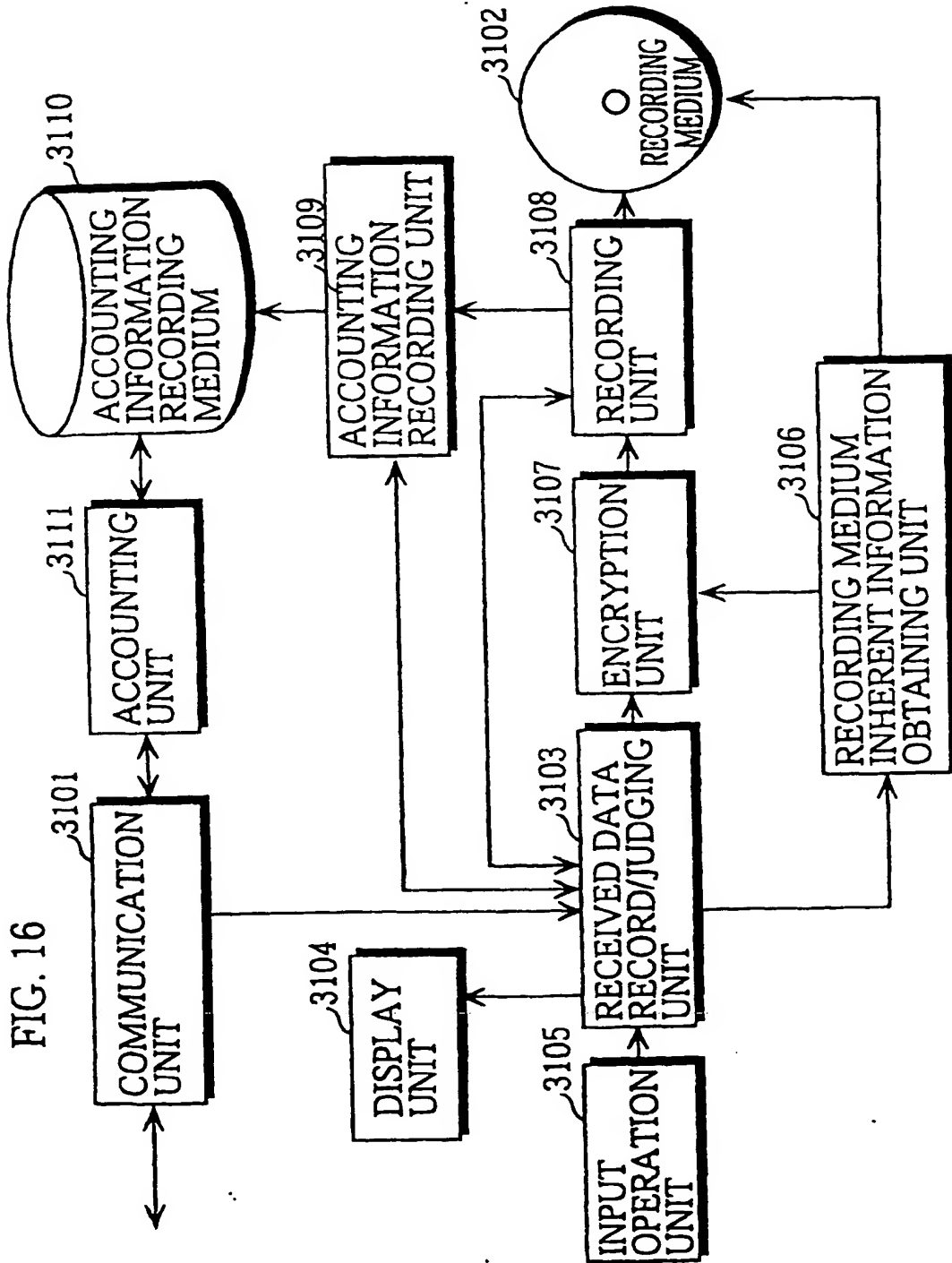


FIG. 17

ATTRIBUTE INFORMATION 3201

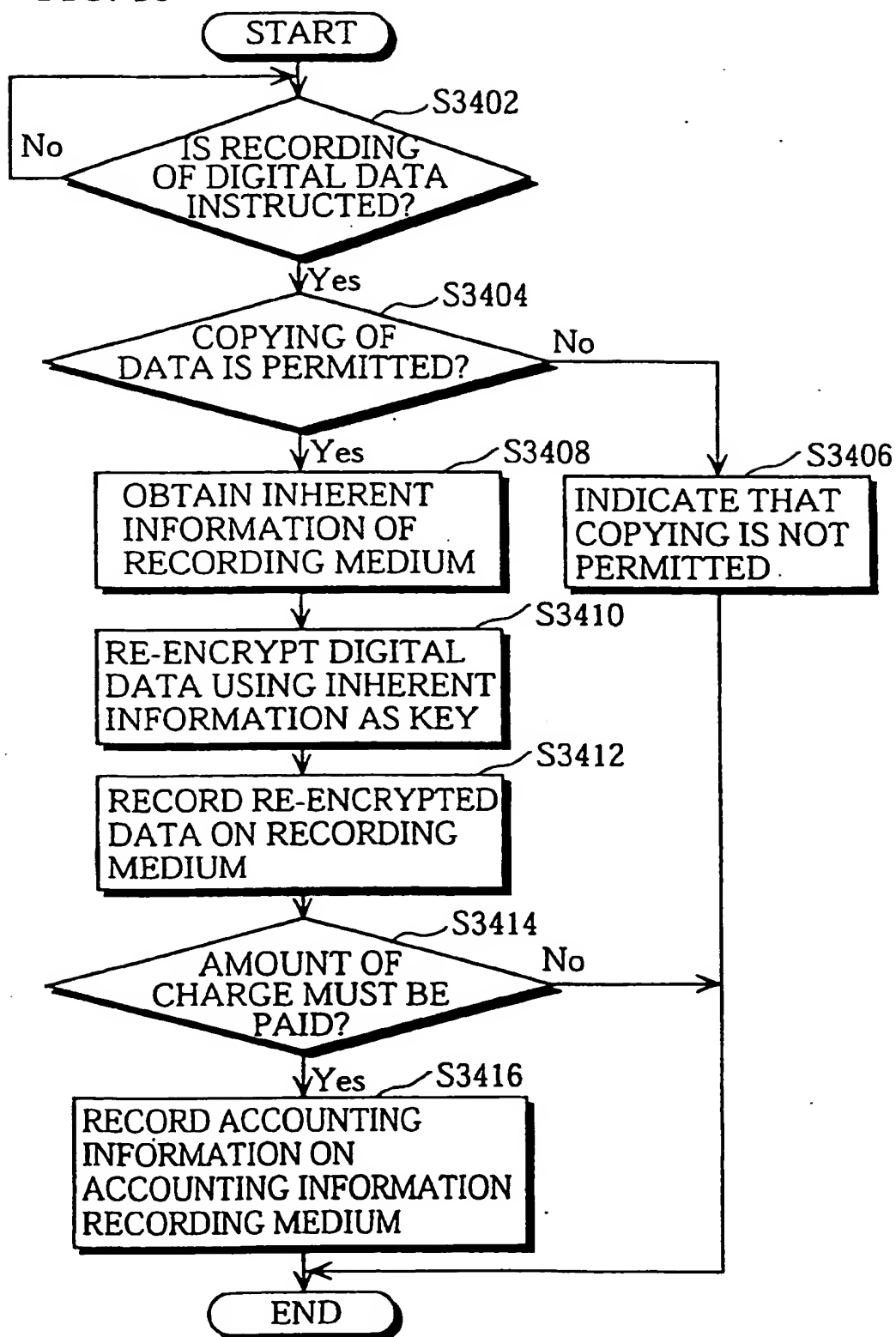
TITLE	PERFORMER	TITLE CODE	RECORDING CHARGE	CHARGE PER REPRODUCTION	MAXIMUM NUMBER OF REPRODUCING	ENCRYPTION CONDITION	COPY PERMISSION	...
MUSIC A	a	song01	¥100	¥0.5	100回	ENCRYPTED	ONLY ONCE	...
MUSIC B	b	song02	¥10	¥0	NO LIMIT	NOT ENCRYPTED	PERMITTED	...
MUSIC C	c	song03	¥0	¥1	50回	ENCRYPTED	ONLY ONCE	...
MUSIC D	d	song04	¥30	¥5	50回	ENCRYPTED	ONLY ONCE	...
MUSIC E	e	song05	¥10	¥0	10回	NOT ENCRYPTED	PERMITTED	...

FIG. 18

MANAGEMENT INFORMATION 3301

TITLE CODE	RECORDING START ADDRESS	RECORDING END ADDRESS
song01	00320	00933
song02	14902	15172
song03	13085	13994
song04	50870	51825
song05	58349	58783

FIG. 19



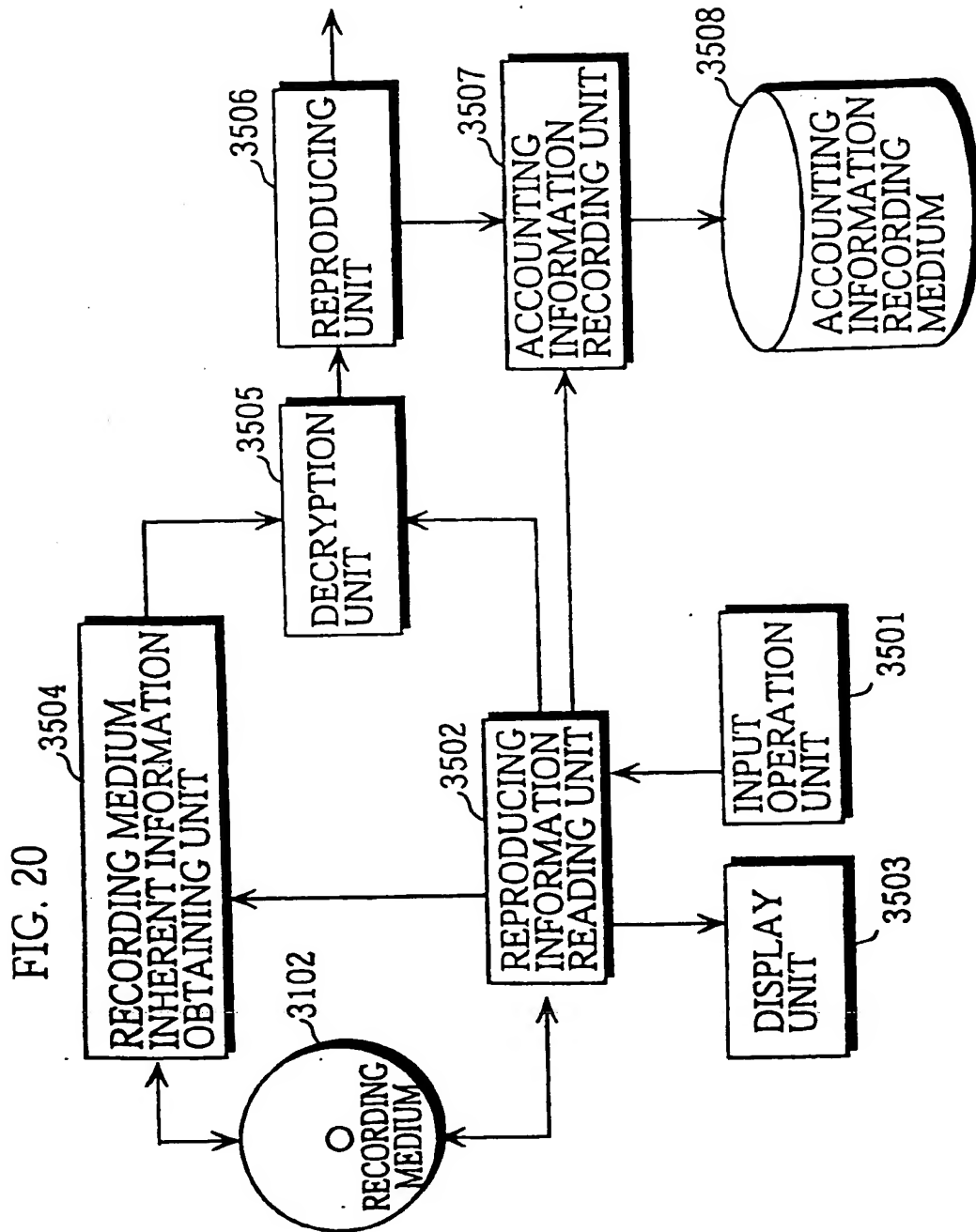


FIG. 21

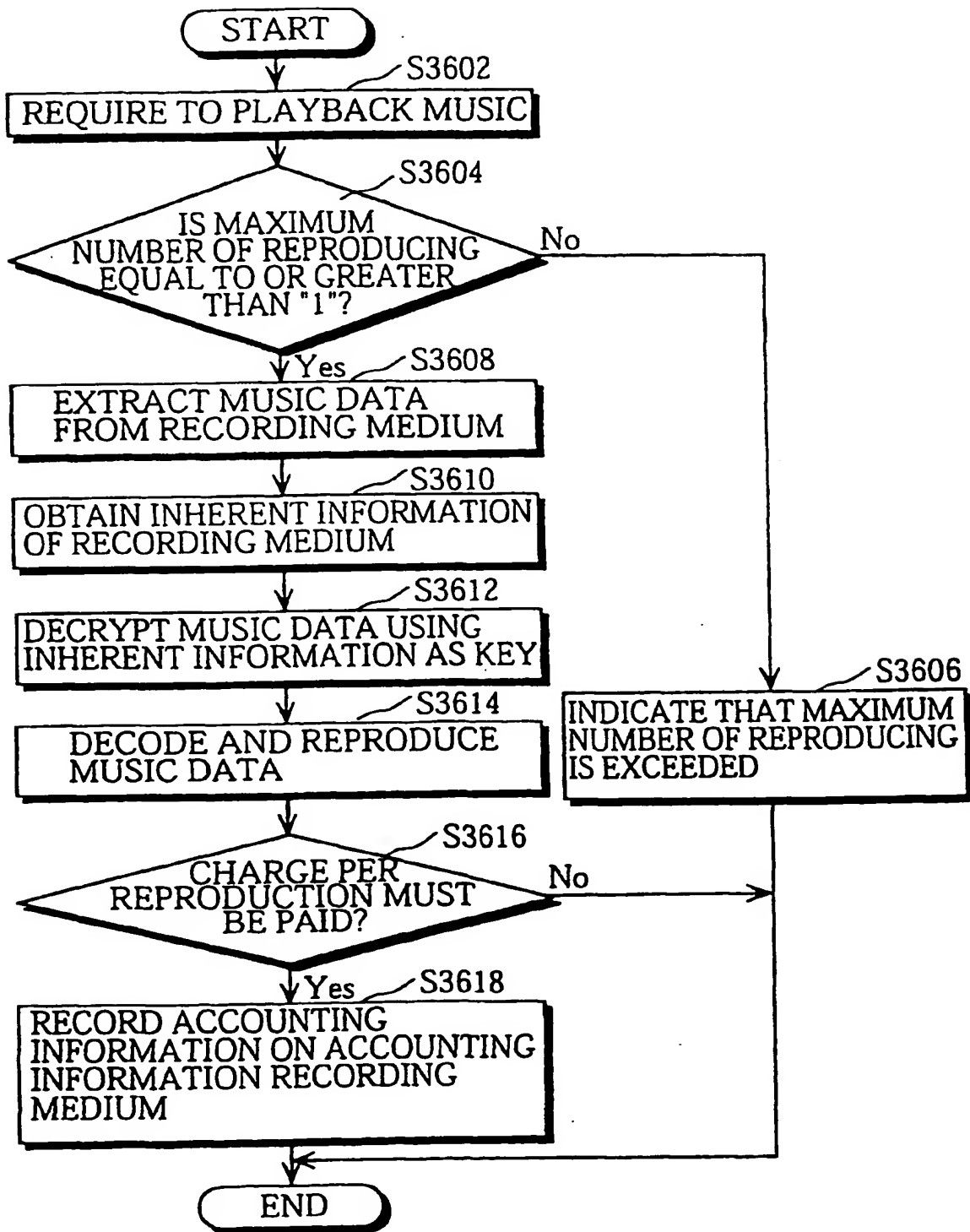


FIG. 22 3700 SECOND DIGITAL DATA RECORDING/PLAYBACK APPARATUS

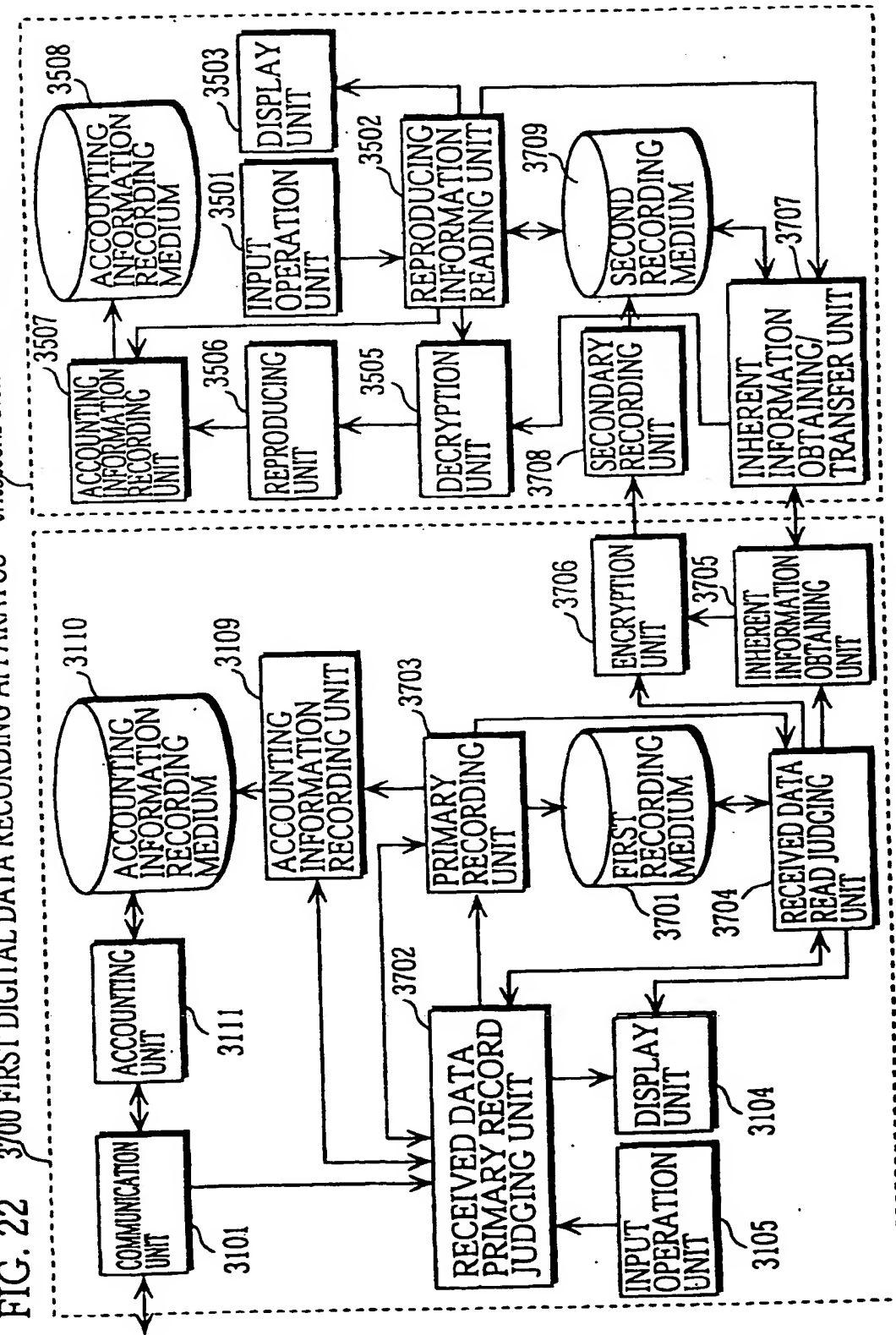


FIG. 23

ATTRIBUTE INFORMATION 3801

		3805		3802		3803				3804
TITLE	PERFOR- MER	TITLE CODE	PRIMARY RECORDING CHARGE	SECONDARY RECORDING CHARGE	CHARGE PER REPRODUCTION	MAXIMUM NUMBER OF REPRODUCING	ENCRYPTION CONDITION	COPY PERMISSION (PRIMARY)	COPY PERMISSION (SECONDARY)	...
MUSIC A	a	song01	¥0	¥100	¥0.5	100回	ENCRYPTED	ONLY ONCE	ONLY ONCE	...
MUSIC B	b	song02	¥10	¥10	¥0	NO LIMIT	NOT ENCRYPTED	PERMITTED	PERMITTED	...
MUSIC C	c	song03	¥0	¥0	¥1	50回	ENCRYPTED	ONLY ONCE	ONLY ONCE	...
MUSIC D	d	song04	¥0	¥30	¥5	50回	ENCRYPTED	ONLY ONCE	ONLY ONCE	...
MUSIC E	e	song05	—	—	—	—	NOT ENCRYPTED	NOT PERMITTED	NOT PERMITTED	...

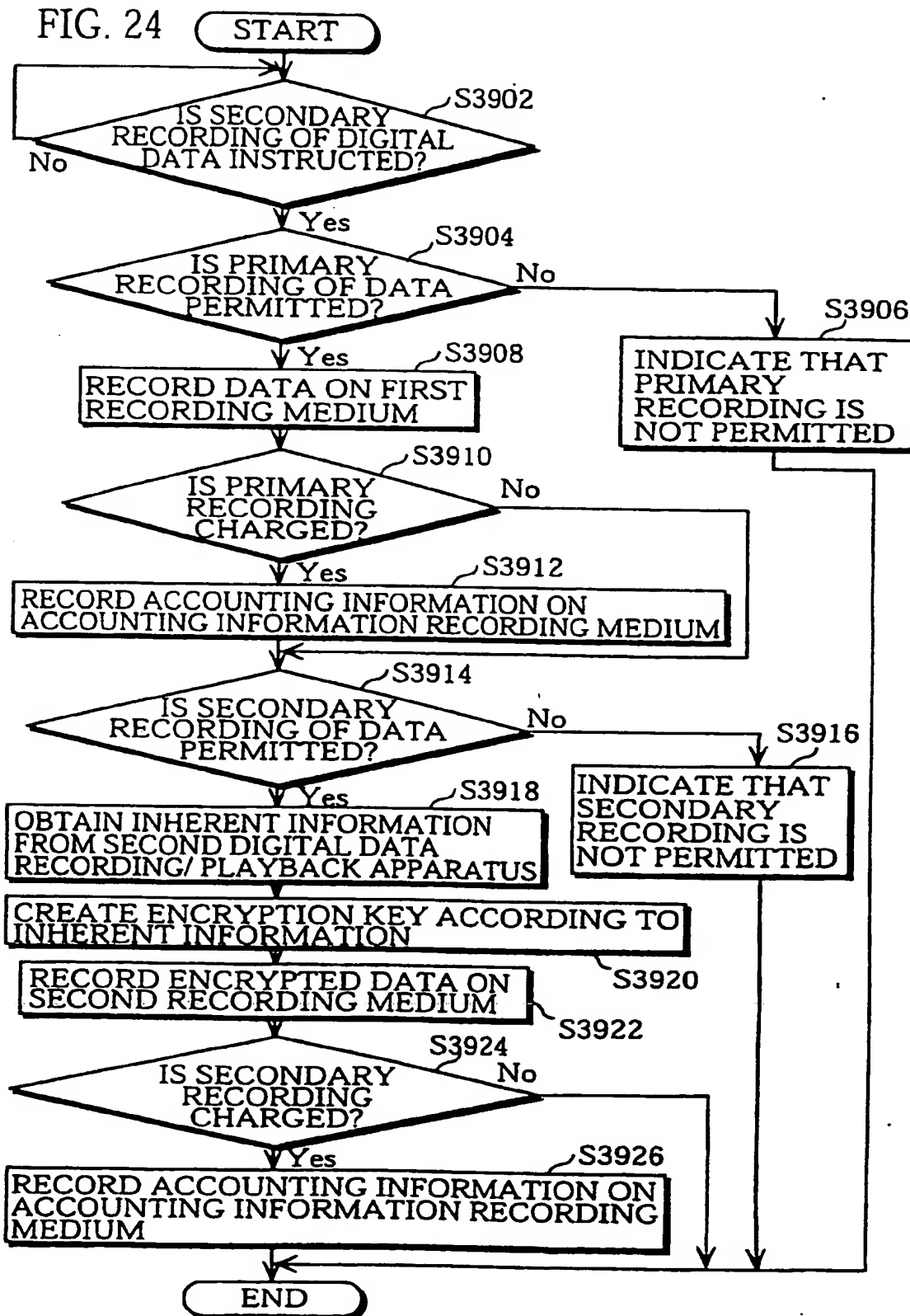


FIG. 25

		31003 31002 31004			31005		ATTRIBUTE INFORMATION 31001	
...	TITLE CODE	...	SECONDARY/RECORDING CHARGE			...		
			MEDIUM ID	APPARATUS ID	MEDIUM ID+ APPARATUS ID			
...	song01	...	¥100	¥10	¥10	...		
...	song02	...	¥10	¥1	¥1	...		
...	song03	...	¥0	¥0	¥0	...		
...	song04	...	¥30	¥3	¥3	...		
...	song05	...	¥10	¥1	¥1	...		

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP99/03887A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl⁶ G11B20/10

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl⁶ G11B20/10Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho 1922-1999 Toroku Jitsuyo Shinan Koho 1994-1999
Kokai Jitsuyo Shinan Koho 1971-1999 Jitsuyo Shinan Toroku Koho 1996-1999

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	JP, 7-272399, A (Hitachi, Ltd.), 20 October, 1995 (20. 10. 95), Full text ; Figs. 1 to 18 & US, 5912969, A	1-12
A	JP, 8-339629, A (Matsushita Electric Industrial Co., Ltd.), 24 December, 1996 (24. 12. 96), Full text ; Figs. 1 to 4 (Family: none)	1-12
P, A	JP, 11-191266, A (Kobe Steel, Ltd.), 13 July, 1999 (13. 07. 99), Full text ; Figs. 1, 2 (Family: none)	1-12

☐ Further documents are listed in the continuation of Box C.
 ☐ See patent family annex.

* Special categories of cited documents:

A document defining the general state of the art which is not considered to be of particular relevance

E earlier document but published on or after the international filing date

I document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

O documents referring to an oral disclosure, use, exhibition or other means

P document published prior to the international filing date but later than the priority date claimed

T later document published after the international filing date or priority date and not in conflict with the application but cited to understate the principle or theory underlying the invention

X document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

Y document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

Z document member of the same patent family

Date of the actual completion of the international search
19 October, 1999 (19. 10. 99)Date of mailing of the international search report
2 November, 1999 (02. 11. 99)Name and mailing address of the ISA/
Japanese Patent Office

Authorized officer

Facsimile No.

Telephone No.

Form PCT/ISA/210 (second sheet) (July 1992)